

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-85015

(43) 公開日 平成11年(1999) 3月30日

(51) IntCl.⁶

識別記号

F I

G 0 9 C 1/00

6 3 0

G 0 9 C 1/00

6 3 0 Z

H 0 4 L 9/08

H 0 4 L 9/00

6 0 1 Z

審査請求 未請求 請求項の数34 O L (全 30 頁)

(21) 出願番号 特願平10-191899

(22) 出願日 平成10年(1998) 7月7日

(31) 優先権主張番号 特願平9-181627

(32) 優先日 平9(1997) 7月7日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(74) 代理人 弁理士 大菅 義之 (外1名)

最終頁に続く

(54) 【発明の名称】 鍵回復システム

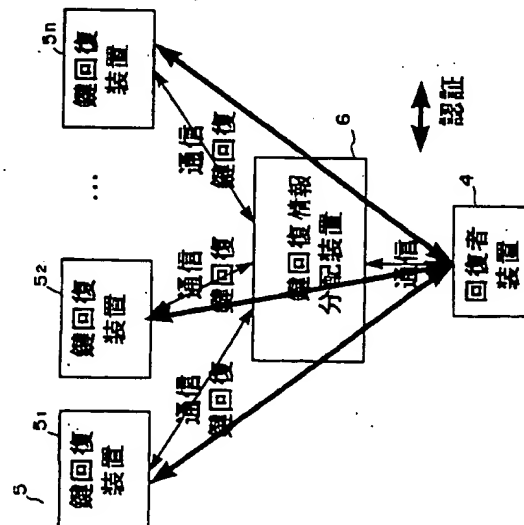
(57) 【要約】

【課題】 回復者装置と鍵回復装置の間に設けられ、鍵情報分配装置が認証データの回復者装置にかわってデータ鍵を回復するとともにその負荷を軽減する。

【解決手段】 データをデータ鍵で暗号化し、鍵回復情報とともに保管しておき、鍵を紛失したとき、暗号の回復者装置が鍵回復情報を鍵回復情報分配装置を介して鍵回復装置に分配して鍵情報を回復し、鍵回復装置と回復者装置との間で直接認証を行ってから鍵情報を回復者装置に転送し、回復者装置でデータ鍵を回復する。

本発明の原理にかか

鍵回復システムの原理を示すブロック図



【特許請求の範囲】

【請求項1】 暗号化データとともに、暗号化したデータ鍵を含む鍵回復情報を格納し、暗号化データに添付してある鍵回復情報からデータ鍵を取り出し、暗号化データを復号する鍵回復システムにおいて、鍵の回復を要求する回復者装置、回復要求に応じて対応する鍵回復装置へ通信路を提供する鍵回復情報分配装置、鍵回復情報からデータ鍵、あるいはその一部を復号して取り出し、回復者の認証を回復者装置と直接行う少なくとも1つの鍵回復装置からなることを特徴とする鍵回復システム。

【請求項2】 前記認証は回復者装置のパスワードの一致を鍵回復装置で判断することにより行われることを特徴とする請求項1記載の鍵回復システム。

【請求項3】 前記認証は回復者装置と鍵回復装置との間で共有されたセッション鍵で暗号化されたメッセージを用いて行うことを特徴とする請求項1記載の鍵回復システム。

【請求項4】 前記鍵回復情報分配装置は、鍵回復装置の認証要求および回復者装置の認証応答を中継する認証情報中継部を有することを特徴とする請求項1記載の鍵回復システム。

【請求項5】 前記データ鍵は、鍵回復装置から取得した公開鍵で暗号化されて鍵回復情報として記憶されるとともに、前記データ鍵は、前記回復者装置の公開鍵で暗号化されて回復者装置に保管され、通常時は、データ鍵で暗号化データを復号するが、該回復者装置の秘密鍵がない場合、前記鍵回復情報を用いてデータ鍵を復号することを特徴とする請求項1記載の鍵回復システム。

【請求項6】 鍵回復情報はさらに鍵回復条件を含み、回復要求を鍵回復情報分配装置を経由して鍵回復装置に伝え、回復条件に従った回復者の認証を鍵回復情報分配装置を経由しながら回復者装置と鍵回復装置が直接行い、認証が有効であった場合は、鍵回復装置が鍵回復情報分配装置を経由しながら鍵情報を回復者装置に送り、回復者装置が鍵情報をもとに鍵を回復することを特徴とする請求項1記載の鍵回復システム。

【請求項7】 鍵回復装置から回復者装置に送られる鍵情報は鍵回復装置と回復者装置との間の共通のセッション鍵で暗号化されていることを特徴とする請求項5記載の鍵回復システム。

【請求項8】 データ鍵に基づくデータの回復を回復者装置で行うことを特徴とする請求項5記載の鍵回復システム。

【請求項9】 認証を回復情報分配装置を介さず回復者装置と鍵回復装置との間の直接接続路を介して行うことを特徴とする請求項5記載の鍵回復システム。

【請求項10】 データ鍵に基づくデータの回復を回復者装置が行うことを特徴とする請求項9記載の鍵回復システム。

【請求項11】 鍵回復情報はさらに鍵回復条件を含み、回復要求を鍵回復情報分配装置を経由して鍵回復装置に伝え、回復条件に従った回復者の認証を鍵回復情報分配装置を経由しながら回復者装置と鍵回復装置が直接行い、認証が有効であった場合は、鍵回復装置から鍵情報を鍵回復情報分配装置が得て、鍵回復情報分配装置が鍵情報を元に鍵を回復し、その鍵を回復者装置に伝えることを特徴とした請求項1記載の鍵回復システム。

【請求項12】 データ鍵に基づくデータの回復を鍵回復情報分配装置で行うことを特徴とする請求項11記載の鍵回復システム。

【請求項13】 認証を回復者装置と鍵回復装置との間で鍵回復情報分配装置を介さず直接接続路を介して行うことを特徴とする鍵回復情報を特徴とする請求項11記載の鍵回復システム。

【請求項14】 データ鍵にもとづくデータの回復を鍵回復情報分配装置において行うことを特徴とする請求項13記載の鍵回復システム。

【請求項15】 鍵回復情報は更に鍵回復装置のIDからなることを特徴とする請求項1記載の鍵回復システム。

【請求項16】 前記鍵回復情報は各鍵回復装置に対して、並列方式に権限分散されることを特徴とする請求項1記載の鍵回復システム。

【請求項17】 前記鍵回復情報は、各鍵回復装置に対して、順序方式により権限分散されて構成されたことを特徴とする請求項1記載の鍵回復装置の鍵回復システム。

【請求項18】 前記回復情報分配装置は鍵回復装置のIDと、各鍵回復装置の名前、そのアクセスアドレス、通信プロトコルの対応テーブルをデータベースとして有することを特徴とする請求項1記載の鍵回復システム。

【請求項19】 暗号文に鍵回復情報を添付して記憶し、鍵回復要求があった場合にはその鍵回復要求を送信し、認証要求を受信した場合に鍵回復者が認証情報を入力して認証返答情報を送信し、鍵情報を受信した場合に鍵を回復する回復者装置と、

鍵回復情報を前記回復者装置から受信した場合にデータベースから鍵回復情報に基づいて鍵回復装置のアクセス情報を取得すると共に鍵回復情報を鍵回復装置へ分配し、認証要求を受信した場合には、前記回復者装置に該認証要求を送信し、この認証要求に応じて、回復者装置から認証応答を受信した場合にこの認証応答を鍵回復装置に送信し、鍵情報を受信した場合にこれを回復者装置に送信する鍵回復情報分配装置と、

鍵回復情報を受信した場合に鍵回復情報から鍵情報を得、この鍵情報を用いて回復条件を復号し、その回復条件に基づく認証要求を回復者装置に前記鍵回復情報分配装置を介して送り、認証応答を回復者装置から受信した場合には認証応答の検証を行うことにより回復者装置と

直接認証を行い、この認証が正しかった場合には鍵情報を鍵回復情報分配装置を介して回復者装置に転送する少なくとも1つの鍵回復装置とからなることを特徴とする鍵回復システム。

【請求項20】 鍵回復情報を回復者装置から鍵回復情報分配装置を介して少なくとも1つの鍵回復装置に分配して鍵を回復する鍵回復システムに用いられ、暗号文を鍵回復情報を添付して記憶し、鍵回復要求があった場合にはその鍵回復要求を送信することにより認証を鍵回復装置と直接行い、認証要求を受信した場合に鍵回復者が10 認証情報を入力して認証返答情報を送信し、鍵情報を受信した場合に鍵を回復することを特徴とする回復者装置。

【請求項21】 鍵回復情報を回復者装置から鍵回復情報分配装置を介して少なくとも1つの鍵回復装置に分配して鍵を回復する鍵回復システムに用いられ、鍵回復情報を回復者装置から受信した場合にデータベースから鍵回復情報に基づいて鍵回復装置のアクセス情報を取得し、認証要求を受信した場合には、回復者装置に該認証要求を送信し、この認証要求に応じて、回復者装置から20 認証応答を受信した場合にこの認証応答を回復装置に送信し、鍵情報を受信した場合にこれを回復者装置に送信することを特徴とする鍵回復情報分配装置。

【請求項22】 鍵回復情報を回復者装置から鍵回復情報分配装置を介して少なくとも1つの鍵回復装置に分配して鍵を回復する鍵回復システムに用いられ、鍵回復情報を受信した場合に鍵回復情報から鍵を得、この鍵を用いて回復条件を復号し、その回復条件に基づく認証要求を鍵回復者装置に送り、認証応答を鍵回復者装置から受信した場合には認証応答の検証を行い、この検証が正し30 かった場合には鍵情報を回復者装置に転送することを特徴とする鍵回復装置。

【請求項23】 データ鍵の回復を要求する回復者装置と、

鍵回復要求に応じて対応する鍵回復装置に通信路を提供する鍵回復情報分配装置と、

鍵回復情報からデータ鍵あるいはデータ鍵情報を復号して取り出す少なくとも1つの鍵回復装置と、

前記回復者装置から前記鍵回復情報分配装置を介して各鍵回復装置に鍵回復情報を送信して、データ鍵と回復条件を回復する手段と、

該回復条件に従って前記回復者装置と前記鍵回復装置が直接認証を行う手段と、

前記認証が成立した場合、前記鍵回復装置で回復されたデータ鍵あるいはデータ鍵情報を回復者装置に送信する手段とからなる鍵回復システム。

【請求項24】 暗号化データとともに、暗号化したデータ鍵と回復条件とからなる鍵回復情報を格納し、前記データ鍵を復号する鍵がないとき、データ鍵の回復を要求する回復者ステップ、回復要求に応じて対応する鍵回40

復ステップへ通信路を提供する鍵回復情報分配ステップ、鍵回復情報からデータ鍵、あるいはその一部を復号して取り出し、回復者の認証を前記鍵回復者ステップと前記鍵回復ステップとで直接行う少なくとも1つの鍵回復ステップからなることを特徴とする鍵回復方法。

【請求項25】 回復要求を鍵回復情報分配ステップを経由して鍵回復ステップに伝え、回復条件に従った回復者の認証を鍵回復情報分配ステップを経由しながら回復者ステップと鍵回復ステップが直接行い、認証が有効であった場合は、鍵回復装置が鍵回復情報分配ステップを経由しながら鍵情報を回復者ステップに送り、回復者ステップが鍵情報をもとに鍵を回復することを特徴とする請求項24記載の鍵回復方法。

【請求項26】 回復要求を鍵回復情報分配ステップを経由して鍵回復ステップに伝え、回復条件に従った回復者の認証を鍵回復情報分配ステップを経由しながら回復者ステップと鍵回復ステップが直接行い、認証が有効であった場合は、鍵回復ステップから鍵情報を鍵回復情報分配ステップが得て、鍵回復情報分配ステップが鍵情報を元に鍵を回復し、その鍵を回復者ステップに伝えることを特徴とした請求項24記載の鍵回復方法。

【請求項27】 暗号文を鍵回復情報を添付して記憶し、鍵回復要求があった場合にはその鍵回復要求を送信し、認証要求を受信した場合に鍵回復者が認証情報を入力して認証返答情報を送信し、鍵情報を受信した場合に鍵を回復する回復者ステップと、
鍵回復情報を前記回復者ステップから受信した場合にデータベースから鍵回復情報に基づいて鍵回復ステップのアクセス情報を取得すると共に、鍵回復情報を鍵回復ステップに分配し、鍵情報を受信した場合にこれを回復者ステップに送信する鍵回復情報分配ステップと、
鍵回復情報を受信した場合に鍵情報を得、この鍵情報を用いて認証要求を回復者ステップに前記鍵回復情報分配ステップを介して送り、認証応答を回復者ステップから受信した場合には認証応答の検証を行い、この検証が正しかった場合には鍵情報を鍵回復情報分配ステップを介して回復者ステップに転送する鍵回復ステップとからなることを特徴とする鍵回復方法。

【請求項28】 鍵の回復を要求する鍵回復者装置と、
鍵回復要求に応じて対応する回復装置に通信路を提供する分配装置と、

鍵回復情報からデータ鍵情報の一部を復号して取り出す少なくとも1つの鍵回復装置を用いて、データ鍵を復号する鍵がない場合にデータ鍵を回復する方法において、
鍵回復者装置から鍵情報分配装置を介して各鍵回復装置に鍵回復情報を送信して、データ鍵と回復条件を回復するステップと、

該回復条件に従って前記回復者装置と前記鍵回復装置が直接認証を行うステップと、

前記認証が成立した場合、前記鍵回復装置で回復された

鍵を回復者装置に送信するステップとからなることを特徴とする鍵回復方法。

【請求項29】 暗号化データとともに、公開鍵で暗号化したデータ鍵と回復条件とからなる鍵回復情報を格納し、通常時は、そのデータ鍵で暗号化データを回復するが、データ鍵なしで復号するために、鍵の回復を要求する回復者機能、回復要求に応じて対応する鍵回復機能へ通信路を提供する鍵回復情報分配機能、鍵回復情報からデータ鍵、あるいはその一部を復号して取り出し、回復者の認証を前記鍵回復者機能と前記鍵回復機能とで直接行う少なくとも1つの鍵回復機能を計算機に行わせることを特徴とする計算機読み出し可能な記録媒体。

【請求項30】 暗号文を鍵回復情報を添付して記憶し、鍵回復要求があった場合にはその鍵回復要求を送信し、認証要求を受信した場合に鍵回復者が認証情報を入力して認証返答情報を送信し、鍵情報を受信した場合に鍵を回復する回復者機能と、鍵回復情報を前記回復者機能から受信した場合にデータベースから鍵回復情報に基づいて鍵回復機能のアクセス情報を取得すると共に鍵回復情報を鍵回復装置に分配し、認証要求を受信した場合には、前記回復者機能に該認証要求を送信し、この認証要求に応じて、回復者機能から認証応答を受信した場合にこの認証応答を回復者機能に送信し、鍵情報を受信した場合にこれを回復者機能に送信する鍵回復情報分配機能と、鍵回復情報を受信した場合に鍵回復情報を得、この鍵情報を用いて認証要求を鍵回復者機能に前記鍵回復情報分配機能を介して送り、認証応答を回復者機能から受信した場合には認証応答の検証を行うことにより回復者機能と直接認証を行い、この検証が正しかった場合には鍵情報を鍵回復情報分配機能を介して回復者機能に転送する鍵回復機能とを計算機に行わせることを特徴とする計算機読み出し可能な記録媒体。

【請求項31】 鍵の回復を要求する回復者機能と、鍵回復要求に応じて対応する鍵回復機能に通信路を提供する鍵回復情報分配機能と、鍵回復情報からデータ鍵情報の一部を復号して取り出す少なくとも1つの鍵回復機能、前記鍵回復者機能から前記鍵回復情報分配機能を介して各鍵回復機能に鍵回復情報を送信して、データ鍵と回復条件を回復する機能と、該回復条件に従って前記回復者機能と前記鍵回復機能が直接認証を行う機能と、前記認証が成立した場合、前記鍵回復機能で回復された鍵を回復者機能に送信する機能とを計算機に行わせることを特徴とする計算機読み出し可能な記録媒体。

【請求項32】 暗号文を鍵回復情報を添付して記憶し、鍵回復要求があった場合にはその鍵回復要求を送信することにより認証を鍵回復機能と直接行い、認証要求を受信した場合に鍵回復者が認証情報を入力して認証返

答情報を送信し、鍵情報を受信した場合に鍵を回復する機能を計算機に行わせることを特徴とする計算機読み出し可能な記録媒体。

【請求項33】 鍵回復情報を回復者機能から受信した場合にデータベースから鍵回復情報に基づいて鍵回復機能のアクセス情報を取得し、認証要求を受信した場合には、回復者機能に該認証要求を送信し、この認証要求に応じて、回復者機能から認証応答を受信した場合にこの認証応答を鍵回復機能に送信することにより認証を回復者機能と鍵回復機能との間で直接行い、鍵情報を受信した場合にこれを回復者機能に送信することにより鍵回復情報分配機能を計算機に行わせることを特徴とする計算機読み出し可能な記録媒体。

【請求項34】 鍵回復情報を受信した場合に鍵回復情報から鍵を得、この鍵を用いて回復条件を復号し、その回復条件に基づく認証要求を回復者機能に送り、認証応答を回復者機能から受信した場合には認証応答の検証を行うことにより認証を回復者機能と鍵回復機能との間で直接行い、この検証が正しかった場合には鍵情報を回復者機能に転送する鍵回復機能計算機に行わせることを特徴とする計算機読み出し可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、例えばデータを鍵で暗号化して暗号文として保管する場合、ユーザの担当者が不在であったり、ユーザの秘密鍵が紛失した時などの緊急時に、暗号文の鍵を回復する鍵回復システムに関する。

【0002】

【従来の技術】鍵回復システムを実現するためには、予め各ユーザの鍵を預けておく方法と、システムの鍵でデータの鍵を暗号化しておく方式がある。本発明は、後者の方式による鍵回復システムである。

【0003】各ユーザは、データを暗号化する場合に、暗号化したデータとともに、データを暗号化した鍵（以下、データ鍵と呼ぶ）を、予め入手したシステム鍵（以下、公開鍵と呼ぶ）で暗号化し、回復条件とともに鍵回復情報として格納する。

【0004】上記公開鍵は、少なくとも1つの鍵回復装置（鍵回復センタともいう）から入手する。ユーザ（回復者装置）が秘密鍵を持っている場合は、データ鍵を自分の公開鍵で暗号化したものを秘密鍵で復号してデータ鍵で暗号化データを復号する。ユーザが秘密鍵を紛失した場合、あるいは緊急に第3者がこの暗号化データを復号する必要がある場合には、データ鍵を鍵回復装置から回復するために暗号化データに添付してある鍵回復情報を取り出し、鍵回復装置に送付する。

【0005】鍵回復装置は、鍵回復情報を参照し、回復者が回復権限を有するか確認し、ある場合は、鍵回復情報からデータ鍵を復元し、回復者に出力する。従来の鍵

回復システムにおいては、鍵回復装置は、秘密鍵を有しているため、その公開鍵で暗号化されたデータ鍵を含む鍵回復情報を添付しているすべての暗号文を回復することができてしまう。これを避けるため鍵回復装置の回復能力を分散させる必要がある。このため、鍵回復装置を複数用意し、複数の鍵回復装置の公開鍵(P1, P2, ...)から鍵回復情報を作成し、回復時には全ての鍵回復装置の合意 $K1 + K2 + \dots$ が得られなければ鍵を回復できないようにする方法が一般的にとられている。

【0006】図22は、従来例として、IBMのSKR (Secure Key Recovery)方式を示す。図22に見られるように鍵回復サービスプロバイダ1を設け、回復者装置2の認証は鍵回復サービスプロバイダ1が行い、その認証が正しければ、鍵回復サービスプロバイダ1が鍵回復情報を複数の鍵回復装置3に送信し、各鍵回復装置3が鍵情報を回復し、その鍵情報から鍵回復サービスプロバイダ1を経由して回復者装置2に鍵を返していた。

【0007】

【発明が解決しようとする課題】図22の従来の方式では、鍵回復サービスプロバイダ1と回復者の間の認証をもとにデータ鍵を回復していたため、暗号文作成者が鍵回復装置毎に回復条件を指定していた場合、鍵回復サービスプロバイダ1は、鍵回復装置に応じた認証処理に対応できない場合があり、オーバーヘッドが大きくなり、場合によっては、鍵回復ができない場合もありえた。

【0008】鍵回復サービスプロバイダ1が回復者の認証をあたかも行ったかのように不正を働いた場合には、全ての暗号文を鍵回復サービスプロバイダ1に回復されてしまう問題が生じる。

【0009】本発明は、回復者装置が全ての鍵回復装置と直接通信しないにもかかわらず、回復者装置と鍵回復装置が直接回復者の認証を行い、その認証を元に回復者装置が最終的に鍵が得られる鍵回復システムを提供することを目的とする。

【0010】

【課題を解決するための手段】上記問題点を解決するために、図22の鍵回復サービスプロバイダの代わりに鍵回復情報分配装置を設ける。鍵回復情報分配装置は、関係する鍵回復装置の全情報を管理し、回復者装置の要求にしたがって回復者装置と鍵回復装置の通信を可能にする。ただし、回復者装置の認証は行わない。回復者装置の認証は、鍵回復装置と回復者装置間で直接行う。この場合、鍵回復情報分配装置は、鍵回復装置と回復装置との通信を提供する。そして、その認証を元に回復者装置が最終的に鍵が得られる鍵回復システムを提供する。すなわち、鍵回復情報分配装置は、回復者装置と鍵回復装置の通信を中継するが、回復者装置の認証は行わず、回復者装置の認証は回復者装置のパスワードの一致の判断

を鍵回復装置で行うことにより実行される。

【0011】請求項1記載の発明によれば、暗号化データとともに、公開鍵で暗号化したデータ鍵を含む鍵回復情報を格納し、通常時は、そのデータ鍵で暗号化データを回復するが、データ鍵を復号する秘密鍵がない場合に、暗号化データに添付してある鍵回復情報からデータ鍵を取り出し、暗号化データを復号することのできる鍵回復システムにおいて、鍵の回復を要求する回復者装置、回復要求に応じて対応する鍵回復装置へ通信路を提供する鍵回復情報分配装置、鍵回復情報からデータ鍵、あるいはその一部を復号して取り出し、回復者の認証を回復者装置と直接行う少なくとも1つの鍵回復装置からなることを特徴とする鍵回復システムである。

【0012】請求項19記載の発明によれば、暗号文を鍵回復情報を添付して記憶し、鍵回復要求があった場合にはその鍵回復要求を送信し、認証要求を受信した場合に鍵回復者が認証情報を入力して認証返答情報を送信し、鍵情報を受信した場合に鍵を回復する回復者装置と、鍵回復情報を前記回復者装置から受信した場合にデータベースから鍵回復情報に基づいて鍵回復装置のアクセス情報を取得し、認証要求を受信した場合には、前記回復者装置に該認証要求を送信し、この認証要求に応じて、回復者装置から認証応答を受信した場合にこの認証応答を鍵回復装置に送信し、鍵情報を受信した場合にこれを回復者装置に送信する鍵回復情報分配装置と、鍵回復情報を受信した場合に鍵回復情報から鍵情報を得、この鍵情報を用いて認証要求を鍵回復者装置に前記鍵回復情報分配装置を介して送り、認証応答を鍵回復者装置から受信した場合には認証応答の検証を行い、この検証が新しかった場合には鍵情報を鍵回復情報分配装置を介して回復者装置に転送する鍵回復装置とからなる鍵回復システムを提供する。

【0013】請求項23の発明によれば鍵の回復を要求する回復者装置と、鍵回復要求に応じて対応する鍵回復装置に通信路を提供する鍵回復情報分配装置と、鍵回復情報からデータ鍵情報の一部を復号して取り出す少なくとも1つの鍵回復装置と、前記鍵回復者装置から前記鍵回復情報分配装置を介して各鍵回復装置に鍵回復情報を送信して、データ鍵と回復条件を回復する手段と、該回復条件に従って前記回復者装置と前記鍵回復装置が直接認証を行う手段と、前記認証が成立した場合、前記鍵回復装置で回復された鍵を回復者装置に送信する手段とからなる鍵回復システムを提供する。

【0014】請求項28記載の発明によれば、鍵の回復を要求する回復者装置と、鍵回復要求に応じて対応する鍵回復装置に通信路を提供する分配装置と、鍵回復情報からデータ鍵情報の一部を復号して取り出す少なくとも1つの鍵回復装置を用いて、データ鍵を復号する鍵がない場合にデータ鍵を回復する方法において、鍵回復者装置から鍵情報分配装置を介して各鍵回復装置に鍵回復情

報を送信して、データ鍵と回復条件を回復するステップと、該回復条件に従って前記回復者装置と前記鍵回復装置が直接認証を行うステップと、前記認証が成立した場合、前記鍵回復装置で回復された鍵を回復者装置に送信するステップとからなることを特徴とする鍵回復方法を提供する。

【0015】請求項29記載の発明によれば、暗号化データとともに、公開鍵で暗号化したデータ鍵と回復条件とからなる鍵回復情報を格納し、通常時は、そのデータ鍵で暗号化データを回復するが、データ鍵なしで復号するために、鍵の回復を要求する回復者機能、回復要求に応じて対応する鍵回復機能へ通信路を提供する鍵回復情報分配機能、鍵回復情報からデータ鍵、あるいはその一部を復号して取り出し、回復者の認証を前記回復者機能と前記鍵回復機能とで直接行う少なくとも1つの鍵回復機能を計算機に行わせることを特徴とする計算機読み出し可能な記録媒体を提供する。

【0016】

【発明の実施の形態】図1は、本発明の原理説明図である。図中、回復者装置4は、回復者が回復する暗号文を指定し、直接、鍵回復装置5から要求される認証条件にそった処理を行い、その認証が正しい場合には、鍵を得るものである。

【0017】回復情報分配装置6は、回復者装置4からの回復要求を受け、鍵回復情報に指定された鍵回復装置5と通信し、鍵回復装置5から要求された回復者への認証要求情報を回復者装置に中継し、鍵回復装置5が回復した鍵情報を回復者装置4に中継するものである。鍵回復装置5は、鍵回復情報分配装置6からの回復要求を受け取り、鍵回復情報分配装置に中継されながら回復者装置4と直接認証情報をやりとりし、その認証が有効であれば、鍵情報を回復するものである。

【0018】まず、たとえば遺言人である暗号作成者が、データ鍵で暗号化された遺言を鍵回復情報とともに回復者装置4に記録する。その暗号文を復号すべき遺言人が秘密鍵を紛失したり、あるいはその遺言書を読む権利のある人が緊急に遺言書を復号する必要があったとする。

【0019】回復者装置4から回復者装置4のID、公開鍵P、データ鍵K、回復条件RCからなる鍵回復情報ID、P(K)、K(RC)を、鍵回復情報分配装置を介して鍵回復装置5のIDを用いてその鍵回復装置5に送り、鍵回復装置5では公開鍵Pに対する秘密鍵Sを使用してデータ鍵Kを復号しそのKを基に回復条件であるRCを復元する。RCとしては鍵回復者のパスワードやID、テキストデータ等が考えられる。そしてRCがパスワードの場合はそのパスワードを用いて鍵回復装置5は回復者装置4に認証要求を行う。回復者装置4はその認証要求に応じて、例えば回復者のパスワードを入力する。そして、鍵回復者のパスワードを鍵回復装置5に送

り、鍵回復条件検証部にある鍵回復者のパスワードと比較し、一致すれば回復者装置と鍵回復装置5とが直接の認証がとれたことになる。その後、鍵回復装置5は鍵情報を回復者装置4に送信する。鍵回復装置5はデータ鍵Kを使って暗号文を復号する。

【0020】本発明では鍵回復装置5から認証応答があった時点で、例えば回復条件であるパスワードが回復者装置4から入力されたものと鍵回復装置5に記憶されたものが一致した事を見る。これにより回復者装置4が直接、鍵回復装置5と認証を行うので、鍵回復情報分配装置が回復者に成り代わって不正に鍵回復の認証を行うことができない。

【0021】さらに本発明では、鍵回復分散機能を持つことで、回復者装置4の鍵回復装置5に関する情報の管理を削減し、さらに、鍵回復装置5と直接認証することにより様々な認証条件に対応可能となるとともに、鍵回復情報分配装置がかかる様々な認証条件に対応しきれないという問題も生じない。

【0022】図2は、本発明の一実施例構成図である。

本発明の鍵回復システム10は、回復者装置11、鍵回復情報分配装置12、鍵回復装置13からなる。

【0023】回復者装置11は、鍵回復要求部11a、認証応答部11b、鍵回復部11c、暗号処理部11d、制御部11e、通信部11fからなる。鍵回復情報取得部11gは鍵回復情報ID、P(K)、K(RC)を取得する。IDは鍵回復装置ID、Pは鍵回復装置から入手した公開鍵、RCは各鍵回復装置の回復条件である。さらに、データ(平文)はデータ鍵Kで暗号化され、そのデータ鍵Kは、回復者装置11の公開鍵で暗号化され、暗号文とされている。そして、暗号文に鍵回復情報が添付されて、回復者装置に保管しておく。

【0024】鍵回復情報分配装置12は、鍵回復情報解析部12a、鍵回復装置情報取得部12b、認証情報中継装置12c、暗号処理部12d、制御部12e、通信部12fからなる。

【0025】鍵回復装置13は、鍵情報取得部13a、回復条件検証部13b、暗号処理部13c、制御部13d、通信部13eからなる。図3は、図2の実施例における回復者装置の動作を示すフローチャートである。通常は回復者装置は自分の秘密鍵で自分の公開鍵で暗号化されたデータ鍵を復号して、このデータ鍵で暗号文を復号する。しかし、鍵回復者が自分の秘密鍵を紛失し、データ鍵を復号できず、したがってデータ鍵を回復する必要がある場合、すなわち鍵回復要求が回復者装置から発生した場合には、その処理を開始する時点で、まず解読すべき暗号文を指定する(ステップS1、S2)。鍵回復要求部11aにおいて鍵回復情報ID、P(K)、K(RC)を取得し(ステップS3)、制御部11eにおいて鍵回復要求メッセージを作成し(ステップS4)、通信部11fにおいて鍵回復要求メッセージを鍵

回復情報分配装置に送信する(ステップS5)。すなわち、鍵回復要求者が自分の秘密鍵を紛失した場合には、鍵回復要求を鍵回復情報分配装置12に送信するものである。

【0026】次に、鍵回復要求ではない場合であって、認証要求である場合は(ステップS6)、認証応答部11bにおいて、認証手段を例えばパスワード、ID:テキストデータ等の中から例えばパスワードがあると認識する(ステップS7)。そして、パスワード入力を鍵回復者に促す(ステップS8)。鍵回復者がパスワードを入力し認証応答部11bがパスワードを含んだパスワード返答メッセージを作成し(ステップS9、10)、通信部11fにおいてパスワード返答メッセージを鍵回復情報分配装置12に送信する(ステップS11)。

【0027】次に、認証要求ではなかった場合には鍵情報かを判断し(ステップS12)、鍵情報である場合には、制御部11fは鍵情報を鍵回復部11cに送る(ステップS13)。鍵情報とは、並列方式の場合、各鍵回復装置から送られてきた鍵、K1、K2、K3、...、Knである。次に、これら鍵情報K1、K2、K3、...、Knからそれらの排他的論理和をとって鍵Kを回復する(ステップS14)。

【0028】なお、今回の実施例は排他的論理和で鍵を合成するが、閾値法など他の鍵分散方式を用いてもよい。次に鍵Kを制御部に送り(ステップS15)、制御部11eは鍵は回復した旨を回復者装置11に伝える(ステップS16)。鍵情報でもなかった場合には、エラー処理を行う(ステップS17)。

【0029】図4は、図2の実施例における鍵回復情報分配装置の動作を示すフローチャートである。まず、暗号文が鍵回復者から送られてきた場合、これが鍵回復情報ID、P(K)、K(RC)であった場合には(ステップS21)、制御部12eを通して鍵回復情報が鍵回復情報解析部12aに送られる(ステップS22)。鍵回復情報解析部12aは個々の鍵回復情報を取り出す(ステップS23)。

【0030】次に、鍵回復情報は制御部12eを通して鍵回復情報取得部12bに送られる(ステップS24)。鍵回復情報取得部12bは鍵回復情報から鍵回復装置13のIDを取得する(ステップS25)。鍵回復情報取得部12bは図10に示す鍵回復装置データベースから鍵回復装置のIDを使ってアクセス方法を取得する(ステップS26)。

【0031】通信部12fはアクセス方法に従って、鍵回復情報を鍵回復装置13に送信する(ステップS27)。次に、鍵回復装置からの認証要求を受信したと判断した場合の動作はステップS28～S31に示す。すなわち、認証要求メッセージを認証情報中継部12cに送る。認証情報中継部12cは認証要求メッセージを通信部12fに送る。認証要求メッセージを鍵回復者装置

11に送る。

【0032】次に鍵回復情報分配装置12が鍵回復者装置11から認証応答を受信したと判断した場合の動作はステップS32～S35に示す。すなわち、認証応答メッセージを認証情報中継部12cに送る。認証情報中継部12cは認証応答メッセージを通信部12fに送る。通信部12fは認証応答メッセージを鍵回復装置13に送る。

【0033】さらに鍵回復情報分配装置12が鍵回復装置11から鍵情報(K1、K2、K3、...、Kn)を受信したと判断した場合の動作をステップS36～S40に示す。すなわち、鍵情報を制御部12eが記憶する。次の鍵回復情報が別の鍵回復装置用に送られてきているか否かを判断し、YESの場合には、その鍵回復情報を制御部12eに送り前述の鍵回復情報を受信した場合の処理に入る。次の鍵回復情報が存在しない時には、鍵情報を通信部12fに送り、鍵情報を回復者装置11の通信部11fに送る。なお、鍵情報を受信した場合でもなかった場合にはエラー処理とする(ステップS41)。

【0034】図5は図2の実施例における鍵回復装置13の動作のフローチャートである。鍵回復装置13が鍵回復情報ID、P(K)、K(RC)を受信した場合の動作をステップS51～S61に示す。すなわち、その鍵回復情報を制御部13dを通して鍵情報取得部13aに送る。鍵回復装置13の秘密鍵Snを不図示の鍵回復装置データベース装置から得る。制御部13dを通して暗号処理を使いながら鍵回復情報の中のPn(Kn)を復号する。そして鍵情報Knを得て制御部13dに送る。制御部13dは暗号化された回復条件Kn(RC)を回復条件検証部13bに送る。回復条件検証部13bは鍵情報Knを用いてKn(RC)を復号する。回復条件検証部13bは回復条件RCとして、パスワードやIDあるいはテキストデータがある中でパスワード認識と認識する。

【0035】次にパスワード要求メッセージを作成する。パスワード要求メッセージを制御部13dを通して通信部13eに送る。通信部13eはパスワード要求メッセージを、すなわち認証要求を鍵回復情報分配装置12に送る。

【0036】次に、鍵回復装置13が受信したデータが鍵回復情報ID、P(K)、K(RC)でなかった場合には、鍵回復者装置11からの認証応答メッセージかを判断する。YESの場合この動作をステップS62～S71に示す。すなわち、制御部13dはパスワード応答メッセージを回復条件検証部13bに送る。パスワード応答メッセージからパスワード①を取得する。登録されているパスワード②を取得する。パスワード①がパスワード②と等しいかを判断し、YESの場合は検証結果を制御部13dに返す。制御部13dは鍵情報メッセージ

を作成し通信部13eに送る。通信部13eは鍵情報メッセージを鍵回復情報分配装置12にすなわちK1, K2...Knを鍵回復情報分配装置12に送る。パスワード①とパスワード②が等しくない場合には、鍵回復装置13からの認証要求に対して、回復者装置11から送られてきた認証応答メッセージが正しくないのであるから、鍵回復装置13は鍵情報を回復者に対して転送することができない。したがって、検証結果を制御部13dにかえし、制御部13dはエラーメッセージを作成し、通信部13eに送る。通信部13eはエラーメッセージを鍵回復情報分配装置12に送り、このエラーメッセージは更に回復者装置11に転送される。

【0037】鍵回復装置が認証応答メッセージを受信した場合でもないものの時にはエラー処理として処理を終了する(ステップS72)。本発明では、図2の如く、鍵回復情報に含まれている鍵回復装置13のIDやアクセス先などの情報を鍵回復情報解析部12a、鍵回復装置情報取得部12bを使って得ることができる。

【0038】従って、回復者装置11は、全ての鍵回復装置13の情報がなくても、直接通信することなく鍵回復情報分配装置12を経由して鍵回復装置13と通信し、データの暗号化に使った鍵を得ることができる。

【0039】また、鍵回復情報分配装置12の認証情報中継部12cがあるので、鍵回復装置13は、認証情報中継部12cを経由して認証要求を回復者装置11に届けることができるので、回復者を直接認証することができる。

【0040】従って、鍵回復サービスを仲介するものがデータ鍵を不正に得ることを防げる。以下に図2に示した本発明の一実施例の全体的動作を説明する。

STEP101:回復者は、回復者装置11の鍵回復要求部11aを用いて、回復する暗号文を指定する。

STEP102:暗号文は、鍵回復要求部11aから制御部11eを通して鍵回復情報取得部11gに送られる。

STEP103:鍵回復情報取得部11gは、暗号文から鍵回復情報を取得する。本実施例の鍵回復情報は、栗田、宮内「公開鍵暗号を用いたファイル鍵暗号」(情報処理学会第47回全国大会P4-197)に示されている。データ鍵Kを鍵回復装置の公開鍵Pで暗号化したP(K)と回復条件RCをデータ鍵Kで暗号化したK(RC)を連結した鍵回復情報P(K), K(RC)①を元にして説明する(ただし、IDは後述する)。なお、P(K), K(RC)で示される鍵回復情報をもとに、鍵回復装置の権限が並列に分散されている鍵回復情報として、P1(K1), K1(RC1), P2(K2), K2(RC2)...Pn(Kn), Kn(RCn)②(並列方式)、鍵回復装置の権限が順序付けされている鍵回復情報として、Pn((Pn-1...P3(P2(P1(K), K(RC1), KC2(RC2)), KC3(RC3))...), KCn(RCn))③(順次方式)を考

慮する。並列方式の鍵回復情報が、順次方式のRC, Kn部分に、順次方式の鍵回復情報が、並列方式のKnの部分に挿入された、並列順次併用方式も考えられる。

STEP104:鍵回復情報取得部11gで得られた鍵回復情報は、制御部11eを通して通信部11fに運ばれ、鍵回復情報分配装置12に送られる。通信手段はHTTPプロトコルなど標準的なプロトコルを使っても良いし、鍵回復システム固有のプロトコルを用いて行われてもよい。また、鍵回復情報分配装置12と回復者装置11間の通信は、暗号処理部11d, 12d、制御手段11e, 12e、通信部11f, 12fによって、ISO1170-3 Information technology-Security techniques-Key management Part3: Mechanisms using asymmetric techniquesに示されるような一般的な方法によって暗号化されてもよい。

STEP105:鍵回復情報分配装置12の通信部12fで受信した鍵回復情報は、制御部12eに送られる。

STEP106:制御部12eは、これを鍵回復情報解析部12aに送る。

STEP107:鍵回復情報解析部12aは、鍵回復情報の形態を識別し、権限分散されている場合には、それぞれの鍵回復装置13の鍵回復情報を抽出する。②の形式の場合には、Pn(Kn), Kn(RCn)がその情報となる。③の形式の場合には、鍵回復装置毎に情報を分けることができないので、そのまま第一の鍵回復装置にあてた鍵回復情報として扱う。

STEP108: STEP105で選ばれた鍵回復情報は、制御部12eに送られ、制御部12eは、鍵回復装置情報取得部12bにおいて、鍵回復装置13へのアクセス方法を得る。鍵回復装置情報取得部12bは、鍵回復装置13の情報をデータベースとしてもっても良いし、鍵回復情報のヘッダ部分から抽出してもよい。鍵回復装置13へのアクセス先は、例えばhttp://kr.ro.jp/などのURLで示されても良いし、/C=jp/o=KR/などのIP=TX.500で示されている識別名などで示されてもよい。

STEP109:制御部12eは、鍵回復情報とアクセス方法を通信部12fに送り、通信部12fは、アクセス方法に従って鍵回復情報を鍵回復装置13に送る。通信手段は、HTTPプロトコルなど標準的なプロトコルを使っても良いし、鍵回復装置固有のプロトコルを用いて行われてもよい。なお、鍵回復情報分配装置12と鍵回復装置13間の通信は、暗号処理部12d, 13c、制御部12e, 13d、通信部12f, 13eによって、ISO1170-3 Information technology-Security techniques - Key management Part3: Mechanisms using asymmetric techniquesに示されるような一般的な方法によって暗号化されてもよい。

STEP110:鍵回復装置13は、通信部13eを通して鍵回復情報を受け取り、通信部13eは、制御部13dを通して鍵回復情報を鍵情報取得部13aに送る。

STEP111:鍵情報取得部13aは、制御部13dを通して暗号処理部13cを用いながら、鍵回復装置13の秘密鍵 S_n を用いて、鍵回復情報 P_n (K_n)を復号し、鍵情報 K_n を得る。この時並列方式の鍵回復情報の場合には、データ鍵 K を秘密化のため分散した鍵の一片が得られ、順次方式の鍵回復情報の場合には、次の鍵回復装置13の公開鍵 P_{n-1} で K_{n-1} と K_n (RC)を暗号化したものが得られる。

STEP112:鍵情報取得部13aで得られた鍵情報は、制御部13dを通して回復条件検証部に送られる。

STEP113:回復条件検証部13bは、制御部13dを通して暗号処理部13cを用いながら、鍵情報を用いて回復条件 RC を復号する。

STEP114:鍵回復条件検証部13bは、復号された回復条件の種類を識別する。回復条件とは、回復者にパスワードを求め、回復者がそのパスワードを答えられれば回復者として認定するものや、回復条件がフリーテキストで書かれたものや、回復者に対する質問と答えが記述されており、質問を回復者に送り、その答えを求めるものや、一般的に知られた公開鍵方式を用いた電子署名のようなものである。本実施例では、パスワードを用いた認証が回復条件として要求されているものとする。

STEP115:回復条件検証部13bは、パスワード要求メッセージを作成する。

STEP116:パスワード要求メッセージは、制御部13d、13eを通して、鍵回復情報分配装置12の通信部12fに送られる。

STEP117:通信部12fは、これを制御部12eに送る。

STEP118:制御部12eは、送られてきた情報がパスワード要求メッセージだと知ると、制御部12eを通して認証情報中継部12cに送る。

STEP119:認証情報中継部12cは、パスワード要求メッセージを制御部12eを通して通信部12fに送り、通信部12fは、パスワード要求メッセージを回復者装置11の通信部11fに送る。

STEP120:通信部11fは、制御部11eを通してパスワード要求メッセージを認証応答部11bに送る。

STEP121:認証応答部11bは、回復者にパスワードの入力を促す。

STEP122:回復者は、認証応答部11bの要求に従いパスワードを入力する。

STEP123:認証応答部11bは、回復者が入力したパスワードをもとにパスワード返答メッセージを作成する。

STEP124:認証応答部11bは、パスワード返答メッセージを制御部11eを通して通信部11fに送る。

STEP125:通信部11fは、パスワード返答メッセージを制御部12eを通して認証情報中継部12cに送る。

STEP126:認証情報中継部12cは、制御手段12eを用いてパスワード返答メッセージを通信部12fに送る。

STEP127:通信部12fは、パスワード返答メッセージを

通信部13eに送る。

STEP128:通信部13eは、制御部13dを通して回復条件検証部13bに送る。

STEP129:回復条件検証部13bは、パスワード返答メッセージ内のパスワードを検証し、その結果を制御部13dに伝える。

STEP130:制御部13dは、検証結果が正しければ鍵情報メッセージを、誤っていればエラーメッセージを通信部13eに送る。

10 STEP131:通信部13eは、鍵情報メッセージ、または、エラーメッセージを通信部12fに送る。

STEP132:通信部12fは、鍵情報メッセージ、または、エラーメッセージを制御部12eに送る。

STEP133:制御部12eは、エラーメッセージならそのまま通信部12f、11fを用いて制御部11eにエラーメッセージを送り処理を完了する。

【0041】鍵情報メッセージであれば、次の鍵回復装置に対する鍵回復情報をSTEP105か

らSTEP131の処理を用いてその鍵回復装置に対する鍵情報を得、この処理が権限分散されている鍵回復装置の数だけ続けられる。

STEP134:STEP132の処理が終わると、制御部12eは、鍵情報を通信部12fを用いて通信部11fに送る。

STEP135:通信部11fは、制御部11eを通して鍵情報を鍵回復部11cに送る。

STEP136:鍵回復部11cは、鍵情報をもとに鍵を回復する。並列方式の場合には、一般的な方法で秘密分散された鍵情報から鍵を回復し、順次方式の場合には、鍵情報が鍵そのものとなる。

30 STEP137:鍵回復部は、鍵を制御手段に送る。

STEP138:制御手段は、鍵をもとに鍵返答メッセージを作成し、通信部12fを通して通信部11fに送る。

STEP139:通信部11fは、鍵返答メッセージを制御部11eに送り、制御部11eは、回復者に鍵が回復した旨を知らせて処理が完了する。

【0042】図6は、本発明に用いられる鍵回復情報の基本フォーマットを示す。すなわち、鍵回復情報は平文(データ)をデータ鍵で暗号文とし、この暗号文に鍵回復情報を添付して回復者装置11に記憶される。そして、鍵回復装置13のID、鍵回復装置13の公開鍵P

40 によってデータ鍵 K を暗号化し、 $P(K)$ および回復条件 RC を例えばパスワードとして回復条件を K で暗号化した $K(RC)$ とからなる。すなわち鍵回復情報はID、 $P(K)$ 、 $K(RC)$ からなり、これが暗号文に添付されている。そして、回復者がデータ鍵を暗号化した自分の公開鍵を復号化する秘密鍵を紛失した場合には、暗号文に添付されている鍵回復情報ID、 $P(K)$ 、 $K(RC)$ を鍵回復情報分散装置12を介して所定の鍵回復装置IDによって指定される鍵回復装置13にアクセスする。そしてその鍵回復装置13から鍵回復情報に含

まれた回復条件として、例えばパスワードによる認証要求が送信されると、回復者装置11がパスワードを入力することにより鍵回復者と鍵回復装置13との間で直接認証を行う。認証が成立した場合にはデータ鍵Kを鍵回復装置13から鍵回復分配装置12を介するか或いは直接回復者装置11に転送するものである。回復者装置11ではこのデータ鍵Kを用いて記憶された暗号文を回復し、平文(データ)を得る。

【0043】図7は並列方式によって権限分散された鍵回復情報を示す図である。この場合、複数の回復者装置が存在し各々鍵回復者装置はID1, ID2, ID3, ... IDnを有しているとする。その時に鍵KをK1, K2, K3, ... Knにそれぞれ分割し、各鍵回復装置の公開鍵でP1, P2, P3, ... Pnでそれぞれの分解された鍵K1, K2, K3, ... Knを暗号化する。そして、暗号文作成者によって定められた認証条件を示す回復条件RC1, RC2, RC3, ... RCnをそれぞれの鍵K1, K2, K3, ... Knで暗号化して、K1(RC1), K2(RC2), K3(RC3), ... Kn(RCn)を作成する。

【0044】このようにして形成された並列方式の鍵回復情報を用いて複数の鍵回復装置に権限分散された場合に鍵回復を以下の如く行う。ID1から鍵回復装置のアクセス方法を得て、P1(K1)K1(RC1)を鍵回復装置ID1に送り秘密鍵S1でP1(K1)を復号し、K1でK1(RC1)を復号する。RC1によって、例えばパスワードを使って認証する。次に後述するようにセッション鍵Ksを回復者装置11と鍵回復装置13との間で共有する。このセッション鍵Ksを使って認証要求あるいは認証応答メッセージを暗号化して認証を行う。これによって回復者装置11と鍵回復装置13との直接認証を行うことができる。すなわち、鍵回復情報分配装置12はこの認証に関与せず、従って従来例のように鍵回復情報分配装置12が回復者になりかわって認証を行うことができず、従ってデータ鍵を得ることができない。次にK1をKsをかけて回復者装置11に戻す。次にID2によって同様の処理を行う。そして、外1を得る。

【0045】

【外1】

$$K1 \oplus K2 \cdots \oplus Kn = K$$

【0046】図8は順次方式に従って権限分散された鍵回復情報を示し、図9は鍵回復装置13の権限が順序付けられて作成された順次方式の鍵回復動作を示すフローチャートを示す。図8及び図9を参照して順次方式を説明する。なお図9のKRIn-1=図8の((Pn-1 · P3 (P2 (P1 (K) K (RC1), KC2 (RC2))K3 (RC3)) ···) KCn (RCn)))である。ここで、KはK=KC1のことと上述のKではない。

【0047】図8において、例えばS3でP3を外すとKR12=P2(P1(K)K(RC1), KC2(RC2)), KC3(RC3)となる。制御部がこのKR12をP2(KR11)=P2(P1(K)K(RC1), KC2(RC2))とKC3(RC3)に分割する。P2(KR11)=P2(P1(K)K(RC1), KC1(RC2))から例えばハッシュ関数をかけてKC3を発生する。KC3でRC3を復号する。これに従って鍵回復装置5が認証をする。認証が正しければ、次にP2(KR11)=P2(P1(K)K(RC1), KC2(RC2))を鍵回復情報分配装置6に送る。この時はセッション鍵Ksは使われない。次にID2を使ってアクセス方法を知ってP2(KR11)=P2(P1(K)K(RC1), KC2(RC2))を鍵回復装置ID2に送る。この装置のS2でP2(P1(K)K(RC1), KC2(RC2))を復号する。P1(K)K(RC1)からハッシュを使ってKC2を得る。KC2によりKC2(RC2)を復号してRC2を得る。RC2により認証を行って認証が成立したらP1(K)K(RC1)を鍵回復情報分配装置6に送り、ID1を使ってアクセス方法を知り、鍵回復装置ID1にP1(K)K(RC1)をS1によってP1(K)を復号しKを得、KによってK(RC1)を復号し、RC1によって認証を行い、認証が成立したらKを鍵回復情報分配装置を介して回復者装置に送る。この時はKはKsで暗号化される。そして、各回復者装置はそれぞれのID1, ID2, ID3, ... IDnを有し、且つそれぞれ回復条件指定RC1, RC2, RC3, ... RCnを有する点も並列方式のフォーマットと同様である。

【0048】なお、上記実施例では、上記鍵回復情報をもとに説明したが、他の形式の鍵回復情報の場合にも本発明の認証を回復者装置と鍵回復装置との間で直接行う方式は採用することができることは述べるまでもない。

【0049】図10は、鍵回復情報分配装置内に設けられたテーブルを示す。このテーブルにおいて鍵回復装置のID毎に回復装置の名前、アクセス先のアドレス、およびそのアクセスのプロトコルがレコードに記憶される。これにより、鍵回復情報から回復装置のIDを取得し、そのIDに基づいて図10に示したテーブルを引くことにより鍵回復情報が示す所定の鍵回復装置をアクセスすることができる。ステップS140~S148はその動作を示す。

【0050】図11は認証情報中継部のフローチャートである。まず処理開始スタート後、認証時に、認証情報中継部が制御部からメッセージを受け取る。そして認証メッセージであった場合には制御部に回復者装置に認証要求メッセージを送ることを要求する。次に制御部が通信部に対して認証要求メッセージの送信指示を行い、通信部が回復者装置に認証要求メッセージを送信する。認証要求メッセージでなかった場合には認証応答メッセー

ジかを判断し、認証応答メッセージの時には制御部に回復装置に認証応答メッセージを送ることを要求する。そして、制御部が通信部に対して認証応答メッセージの送信指示をし、通信部が回復装置に認証要求メッセージを送信する。認証応答メッセージでもない場合には、エラー処理を行う。

【0051】また、回復条件検証部13bの制御フローは前述の図5で点線で示したステップパスワードの一致を見るステップのステップと同一であるので説明を省略する。

【0052】次に、回復者装置の暗号処理部および回復者装置の暗号処理部11d、13cのフローチャートを図12、13を参照して説明する。図12において回復者装置の暗号処理部11dは制御部11cからデータが送られてきた時鍵回復情報が並列方式で構成されている場合には、 $K1, K2, K3, \dots, Kn$ かを判断する(ステップS151、S152)。そして、YES場合には各 $K1 \sim Kn$ の排他的論理和を計算し、鍵 K を計算し、 K を制御部11cに返す処理を行う(ステップS153、S154)。もし、制御部11cからのデータが $K1, K2, K3, \dots, Kn$ でない場合には、通信のためのセッション鍵 Ks の共有処理動作を行い、あるいはセッション鍵 Ks での復号通信処理を行う。

【0053】図13において、鍵回復装置13の暗号処理部13cの動作を示すと、制御部13dからデータが送られてくると(ステップS161)、先ず、データが $Pn(Kn)$ かを判断し、YESであれば、鍵回復情報の鍵情報が並列方式で構成されている場合である。この時の動作はステップS161～S165に示す。即ち回復装置の秘密鍵 Sn を回復者装置のデータベースから取り出し、鍵回復装置の秘密鍵 Sn で $Pn(Kn)$ を復号し、 Kn を得る。そして、 Kn を制御部に返す。

【0054】次に、 $Pn(Kn)$ でない場合には鍵回復情報の鍵情報が順次方式で構成されている場合である。このときの動作はステップS166～S169である。データが $Pn(KRIn-1)$ かを判断する。ここで、 $KRIn-1$ は次の鍵回復装置の鍵回復情報のことである。その判断がYESであれば、鍵回復装置の秘密鍵 Sn を回復者装置のデータベースから取り出し、鍵回復装置の秘密鍵 Sn で $Pn(KRIn-1)$ を復号し $KRIn-1$ を得る。そして、 $KRIn-1$ を制御部13dに返す。

【0055】次に、データが順次方式による鍵回復情報の鍵情報でもない場合には、データが並列方式における回復条件であるかを判断する(ステップS170～S172)。すなわちデータが $Kn, Kn(RCn)$ かを判断する。その結果YESの場合には、 Kn で $Kn(RCn)$ を復号し、 RC を得、 RCn を制御部に返す。さらに、データが並列方式の鍵回復条件出もない場合にはデータが順次方式の鍵回復条件であるかを判断する(ステ

ップS173～S175)。すなわちデータが $Kn, Kn(RCn)$ かを判断する。その結果YESである場合には、 Kn で $Kn(RCn)$ を復号し、 RCn を得る。そして、 RCn を制御部13aに返す。次にデータが順次方式の鍵回復条件でもない場合には、次に通信のためのセッション鍵 Ks の共有処理およびセッション鍵 Ks での暗号通信処理に移行する。

【0056】次に図12、図13を参照して回復者装置と鍵回復装置の間での通信のためのセッション鍵 Ks の共有化処理と、セッション鍵 Ks での暗号通信処理を次に説明する。

【0057】セッション鍵 Ks の共有処理は、回復者の公開鍵 Pr と、鍵回復装置の公開鍵 Pn を用いて行い、その後セッション鍵 Ks を使ってデータを暗号化して回復者装置と鍵回復装置との間で送受信する。暗号通信処理は、通信でのやりとりされるデータをDATAと示し、 Ks で暗号、復号する対称的な処理である。

【0058】セッション鍵 Ks の共有では、

1. 鍵回復装置が $Pr(Ks, R1)$ を作成、送信
 2. 回復者装置は、 $Pr(Ks, R1)$ を復号、 $Ks, R1'$ を得る
 3. 回復者装置が $R1'$ と乱数 $R2$ を鍵回復装置の Pn で暗号化して $Pn(R1', R2)$ を作成。 $Pn(R1', R2)$ を送信
 4. 鍵回復装置が $Pn(R1', R2)$ を復号して、 $R1', R2$ を得て、鍵回復装置が作成した $R1$ と復号し得られた $R1'$ を比較し、合っていれば回復者として認証され、 Ks を暗号通信に利用
 5. 鍵回復装置が4で得られた $R2$ を $Pr(R2)$ として暗号化、送信
 6. 回復者装置が $Pr(R2)$ を復号して得られた情報を $R2'$ として、回復者装置が発生した $R2$ と $R2'$ が同じであれば鍵回復装置が認証でき、 Ks で暗号通信を行う
- という処理を示す。

【0059】より具体的には、図13に示す鍵回復装置13の暗号処理のフローチャートのステップS181～S185において、暗号通信要求かを判断し、YESの場合には回復者の公開鍵 Pr をデータベースであるDBから取り出す。乱数を2つ発生させそれぞれセッション鍵 Ks 、認証子 $R1$ とおく。次に $Pr(Ks, R1)$ を作成し、 $Pr(Ks, R1)$ を制御部13dに返す。 $Pr(Ks, R1)$ は、鍵回復装置から鍵情報分配装置を介して回復者装置に送信する。

【0060】次に、図12の回復者装置11の暗号処理部11dのフローチャートのステップS186～S191に移り、データが $Pr(Ks, R1)$ かを判断し、そうである場合には、回復者の秘密鍵 Sr および鍵回復装置の公開鍵 Pn をデータベースから取り出す。 Sr で $Pr(Ks, R1)$ を復号し、 $Ks, R1$ を得、 Ks を

メモリ保存する。乱数R2を発生し、R1'、R2を回復装置の公開鍵Pnで暗号化し、Pn(R1', R2)を作成し、Pn(R1', R2)を制御部に返す。

【0061】次に、図13の鍵回復装置13のフローチャートのステップS194～S196に移り、Pn(R1', R2)かを判断する。YESの場合には鍵回復装置の秘密鍵Sn、回復者の公開鍵Prを鍵回復装置のDBから取り出す。次にPn(R1/R2)をSnで復号し、R1'、R2を得る。次にR1=R1'かを判断し、これにより回復者が正当な回復者であるかを確認

する。YESであった場合には、Pr(R2)を作成し、制御部にKs、Pr(R2)を返し、Ksで暗号処理指示を行ってPr(R2)を回復者装置に送信する。
【0062】次に、再度鍵情報分配装置を介して回復者装置の暗号処理フローチャートのステップS197～S201)に処理に移り、Pr(R2)かを判断し、YESの場合には回復者の秘密鍵Srをデータベースから取り出し、Rr(R2)をSrで復号し、R2を得る。R2=R2'かを判断しYESの場合は回復者装置が正当な回復者装置であったことが認証されて制御部にKsで

暗号通信指示を行う。今までの処理によって回復者装置および鍵回復装置間の認証が成立し、且つ通信のためのセッション鍵Ksが回復者装置および鍵回復装置において共有されたことになる。

【0063】次に、回復者装置11におけるデータをセッション鍵Ksで暗号通信を行う過程について説明する。ここで、データとは、この例えばパスワード要求メッセージ、パスワード応答メッセージおよびデータ鍵情報K1、K2、K3、・・・Knである。
【0064】先ず、ステップS210～S212'にお

いてKs(DATA)かを判断し、そうである場合はKsをメモリから得て、KsでKs(DATA)を復号しデータを得、そしてデータを制御部11eに返す。次に、ステップS213～S215においてDATAであるかを判断し、YESの場合にはKsをメモリから得て、DATAをKsで暗号し、Ks(DATA)を作成し、Ks(DATA)を制御部11eに返す。すなわち回復者装置11の暗号処理部11dにおいてKs(DATA)は認証要求メッセージを受信あるいは鍵情報K1、K2、K3、・・・Knを受信した場合である。また、DATAかは認証応答メッセージを送信する場合である。

【0065】鍵回復装置13においてもセッション鍵Ksで暗号通信処理を行う場合の処理は図13のフローチャートのステップS216～S224に示される。Ks(DATA)か或いはDATAかは回復者装置11のKs(DATA)かでの暗号通信処理と同様であるから省略する。但し、鍵回復装置13においてはKs(DATA)はパスワード応答メッセージを受信した場合にYESとなり、DATAはパスワード要求メッセージを送信

する場合にYESとなる点異なる。

【0066】上述したように、Ks(DATA)は回復者装置11と鍵回復装置13との間で直接転送される。鍵回復装置と回復者装置との間の認証は両者で共有されたセッションキーKsで暗号化されたメッセージを通信することにより行われる。一方セッションキーKsは鍵情報分配装置では共有されていない。鍵情報分配装置は認証に参加し、メッセージの中身をみ、あるいはメッセージを改ざんすることができない。したがって、回復者は回復者装置と鍵回復装置の間で直接認証される。

【0067】図14は本発明の他の実施例であり、鍵回復部22dを鍵回復情報分配装置22に設けたものである。鍵回復システム20は、回復者装置21、鍵回復情報分配装置22、鍵回復装置23からなる。

【0068】回復者装置21は、鍵回復要求部21a、認証応答部21b、暗号処理部21d、制御部21e、通信部21fからなる。鍵回復情報分配装置22は、鍵回復情報解析部22a、鍵回復装置情報取得部22b、認証情報中継装置22c、鍵回復部21d、暗号処理部22e、制御部22f、通信部22gからなる。

【0069】鍵回復装置23は、鍵情報取得部23a、回復条件検証部23b、暗号処理部23c、制御部23d、通信部23eからなる。

STEP301:回復者は、回復者装置21の鍵回復要求部21aを用いて、回復する暗号文を指定する。

STEP302:暗号文は、鍵回復要求部21aから制御部21eを通して鍵回復情報取得部21cに送られる。

STEP303:鍵回復情報取得部21cは、暗号文から鍵回復情報を取得する。本実施例の鍵回復情報は、栗田、宮内「公開鍵暗号を用いたファイル鍵暗号」(情報処理学会第47回全国大会P4-197)に示されている。データ鍵Kを鍵回復装置の公開鍵Pで暗号化したP(K)と回復条件RCを鍵Kで暗号化したK(RC)を連結した鍵回復情報P(K)、K(RC)①を元にして説明する(ただし、IDは後述する)。なお、R(K)、K(RC)で示される鍵回復情報をもとに、鍵回復装置の権限が並列に分散されている鍵回復情報として、P1(K1)、K1(RC)、P2(K1)、K2(RC2)・・・Pn(Kn)、Kn(RCn)②(並列方式)、鍵回復装置の権限が順序付けされている鍵回復情報として、Pn((Pn-1・・・P3(P2(P1(K)、K(RC1)、KC2(RC2))), KC3(RC3)))・・・), KCn(RCn))③(順次方式)を考慮する。並列方式の鍵回復情報が、順次方式のRC、Kn部分に、順次方式の鍵回復情報が、並列方式のKnの部分に挿入された、並列順次併用方式も考えられる。

STEP304:鍵回復情報取得部21cで得られた鍵回復情報は、制御部21eを通して通信部21fに運ばれ、鍵回復情報分配装置22に送られる。通信手段はHTTPプロトコルなど標準的なプロトコルを使っても良いし、鍵

回復システム固有のプロトコルを用いて行われてもよい。また、鍵回復情報分配装置22と回復者装置21間の通信は、暗号処理部21d、22e、制御部21e、22f、通信部21f、22gによって、ISO1170-3 Information technology-Security techniques-Key management Part3: Mechanisms using asymmetric techniquesに示されるような一般的な方法によって暗号化されてもよい。

STEP305:鍵回復情報分配装置22の通信部22gで受信した鍵回復情報は、制御部22fに送られる。

STEP306:制御部22fの出力は、鍵回復情報解析部22aに送られる。

STEP307:鍵回復情報解析部は、鍵回復情報の形態を識別し、権限分散されている場合には、それぞれの鍵回復装置23の鍵回復情報を抽出する。②の形式の場合には、 $P_n(K_n)$ 、 $K_n(RC_n)$ がその情報となる。③の形式の場合には、鍵回復装置毎に情報を分けることができないので、そのまま第一の鍵回復装置に於て鍵回復情報として扱う。

STEP308: STEP305で選ばれた鍵回復情報は、制御部22fに送られ、制御部22fは、鍵回復装置情報取得部22bにおいて、鍵回復装置へのアクセス方法を得る。鍵回復装置情報取得部22bは、鍵回復装置の情報をデータベースとしてもっても良いし、鍵回復情報のヘッダ部分から抽出してもよい。鍵回復装置23へのアクセス先は、例えばhttp://kr.ro.jp/などのURLで示されても良いし、/C=jp/o=KR/などのITU-TX.500で示されている識別名などで示されても良い。

STEP309:制御部22fは、鍵回復情報とアクセス方法を通信部22gに送り、通信部22gは、アクセス方法に従って鍵回復情報を鍵回復装置23に送る。通信手段は、HTTPプロトコルなど標準的なプロトコルを使っても良いし、鍵回復装置固有のプロトコルを用いて行われてもよい。なお、鍵回復情報分配装置22と鍵回復装置23間の通信は、暗号処理部22e、23c、制御部22f、23d、通信部22g、23eによって、ISO1170-3 Information technology-Security techniques - Key management Part3: Mechanisms using asymmetric techniquesに示されるような一般的な方法によって暗号化されてもよい。

STEP310:鍵回復装置23は、通信部23eを通して鍵回復情報を受け取り、通信部23eは、制御部23dを通して鍵回復情報を鍵情報取得部23aに送る。

STEP311:鍵情報取得部23aは、制御部23dを通して暗号処理部23cを用いながら、鍵回復装置23の秘密鍵 S_n を用いて、鍵回復情報 $P_n(K)$ を復号し、鍵情報 K_n を得る。この時並列方式の鍵回復情報の場合は、鍵 K を秘密分散した鍵の一片が得られ、順次方式の鍵回復情報の場合には、次の鍵回復装置23に対する鍵回復情報と、その情報から生成される鍵で暗号化された回復

条件が得られる。

STEP312:鍵情報取得部23aで得られた鍵情報は、制御部23bを通して回復条件検証部23bに送られる。

STEP313:回復条件検証部23bは、制御部23dを通して暗号処理部23cを用いながら、鍵情報を用いて回復条件 RC を復号する。

STEP314:鍵回復条件検証部23bは、復号された回復条件の種類を識別する。回復条件とは、回復者にパスワードを求め、回復者がそのパスワードを答えられれば回復者として認定するものや、回復条件がフリーテキストで書かれたものや、回復者に対する質問と答えが記述されており、質問を回復者に送り、その答えを求めるものや、一般的に知られた公開鍵方式を用いた電子書名のようなものである。本実施例では、パスワードを用いた認証が回復条件として要求されているものとする。

STEP315:回復条件検証部23bは、パスワード要求メッセージを作成する。

STEP316:パスワード要求メッセージは、制御部23d、通信部23eを通して、鍵回復情報分配装置22の通信部22gに送られる。

STEP317:通信部22gは、これを制御部22fに送られる。

STEP318:鍵回復情報解析部22aは、送られてきた情報がパスワード要求メッセージだと知ると、制御部22fを通して認証情報中継部22cに送る。

STEP319:認証情報中継部22cは、パスワード要求メッセージを制御手段22fを通して通信部22gに送り、通信部22gは、パスワード要求メッセージを回復者装置21の通信部21fに送る。

STEP320:通信部21fは、制御部21eを通してパスワード要求メッセージを認証応答部21bに送る。

STEP321:認証応答部21bは、回復者にパスワードの入力を促す。

STEP322:回復者は、認証応答部21bの要求に従いパスワードを入力する。

STEP323:認証応答部21bは、回復者が入力したパスワードをもとにパスワード返答メッセージを作成する。

STEP324:認証応答部21bは、パスワード返答メッセージを制御部21fを通して通信部21fに送る。

STEP325:通信部21fは、パスワード返答メッセージ制御部22fを通して認証情報中継部22cに送る。

STEP326:認証情報中継部22cは、制御手段22fを用いてパスワード返答メッセージを通信部22gに送る。

STEP327:通信部22gは、パスワード返答メッセージを通信部23eに送る。

STEP328:通信部23eは、制御部23dを通して回復条件検証部23bに送る。

STEP329:回復条件検証部23bは、パスワード返答メッセージ内のパスワードを検証し、その結果を制御部23dに伝える。

STEP330:制御部23dは、検証結果が正しければ鍵情報メッセージを、誤っていればエラーメッセージを通信部23eに送る。

STEP331:通信部23eは、鍵情報メッセージ、または、エラーメッセージを通信部22gに送る。

STEP332:通信部22gは、鍵情報メッセージ、または、エラーメッセージを制御部22fに送る。

STEP333:制御部22fは、エラーメッセージならそのまま通信部22g、21fを用いて制御部21eにエラーメッセージを送り処理を完了する。

STEP334:鍵情報メッセージであれば、次の鍵回復装置23に対する鍵回復情報をSTEP305からSTEP321の処理を用いて処理しその鍵回復装置23に対する鍵情報を得、この処理が権限分散されている鍵回復装置の数だけ続けられる。

STEP335:STEP332の処理が終わると、制御手段22fは、鍵情報を通信部に送る。

STEP336:鍵回復部22dは、鍵情報をもとに鍵を回復する。並列方式の場合には、一般的な方法で秘密分散された鍵情報から鍵を回復し、順次方式の場合には、鍵情報か鍵そのものとなる。

STEP337:鍵回復部22dは、鍵を制御部22fに送る。

STEP338:制御部22fは、鍵をもとに鍵返答メッセージを作成し、通信部22gを通して通信部21fに送る。

STEP339:通信部21fは、鍵返答メッセージを制御部21eに送り、制御部21eは、回復者に鍵が回復した旨を知らせて処理が完了する。

【0070】図15は、鍵回復部を回復者装置に設けた実施例において、認証動作を鍵回復情報分配装置を介さず鍵回復装置と回復者装置とを直接接続して行う実施例である。

【0071】図16は、鍵回復部を鍵回復情報分配装置に設けた実施例において、認証動作の際に鍵回復情報分配装置を介さず鍵回復装置と回復者装置とを直接接続して行う実施例である。

【0072】図17は、鍵回復部とデータ回復部を回復者装置に設けた実施例である。図18は、鍵回復部とデータ回復部を回復者装置に設けた実施例において、認証動作を鍵回復装置と回復者装置とを直接接続して行う実施例である。

【0073】図19は、データ回復部と鍵回復部を鍵回復情報分配装置に設けた実施例である。図20は、図19の実施例において、認証動作を鍵回復装置と回復者装置とを直接接続して行う実施例である。

【0074】図15～図20において、各構成要素は図14と対応した参照符号を付し、より詳細な説明は省略する。なお、図2のように認証動作を鍵回復情報分配装置を介して行う場合は、回復者装置が鍵回復情報を鍵回復装置に送出した時点で通信路が確立しているので、鍵回復装置からの認証要求は、鍵回復装置に鍵回復を要求し

た回復者装置との既に確立された通信路をもって行うことができる。回復者装置と鍵回復装置の認証のため通信を鍵回復情報分配装置を介さずに行くと、回復者装置に対して鍵回復装置が認証要求をする際の通信路を新たに確立しなければならないので、鍵回復装置が回復者装置を呼びにいった場合に回復者装置が話し中等の状態を生ずることがある。

【0075】図21は、本発明の鍵回復システムを実現する情報処理装置（コンピュータ）の構成図である。CPU（中央処理装置）431、メモリ432、入力装置433、出力装置434、外部記憶装置435、媒体駆動装置436、ネットワーク接続装置437を備え、それらの各装置はバス438により互いに結合されている。

【0076】CPU431は、メモリ432に格納されたプログラムを実行する。メモリ432には、上述のプログラムの他に、処理に用いられるデータが格納されている。メモリ432としては、例えばROM（read only memory）、RAM（random access memory）等が用いられる。

【0077】入力装置433は入力装置11に対応し、例えばキーボード、ポインティングデバイス等に相当する。また、出力装置434は出力装置417に対応し、表示装置やプリンタ等に相当する。

【0078】外部記憶装置435は、例えば、磁気ディスク装置、光ディスク装置、光磁気ディスク装置等である。この外部記憶装置435に、上述のプログラムとデータを保存しておき、必要に応じて、それらをメモリ432にロードして使用することができる。また、外部記憶装置435は、データベースとしても使用できる。

【0079】媒体駆動装置436は、可搬記録媒体439を駆動し、その記憶内容にアクセスする。可搬記録媒体439としては、メモ리카ード、フロッピーディスク、CD-ROM（compact disk read only memory）、光ディスク、光磁気ディスク等、任意のコンピュータ読み取り可能な記録媒体を使用することができる。この可搬記録媒体439に、上述のプログラムとデータを格納しておき、必要に応じて、それらをメモリ432にロードして使用することができる。

【0080】ネットワーク接続装置437は、LAN（local area network）等の任意の通信ネットワークに接続され、通信に伴うデータ変換等を行う。また、実施例は遺言書を例にとって、データ鍵Kを暗号化している秘密鍵を紛失し、それを鍵回復装置を用いて回復する場合について述べたが、本発明は遺言書の回復等の用途に用いられるだけでなく、通常の会社等においても使われることは勿論である。例えば会社の総務部において、秘密情報を暗号化させて保管しておいた場合に、その暗号化したデータ鍵Kを暗号化する公開鍵に対応する秘密鍵を紛失したり、あるいはその担当者が不在であるとき

に使用できる。さらには本発明は個人間の通信において暗号化データを通信しあう場合にも用いることができる。

【0081】

【発明の効果】以上説明したように、本発明によれば、鍵回復情報分配装置があるため、回復装置が全ての鍵回復装置を知らなくとも権限分散した鍵回復装置にアクセスでき、且つ、回復者の認証を行うにあたって、回復者装置と鍵回復装置間の認証を直接２者間で行った上で鍵回復装置が回復者装置に鍵を返送可能となる効果を奏し、鍵回復サービスを仲介するサービスプロバイダなどの不正を防ぐことが出来、鍵回復システムにおけるセキュリティ向上に寄与するところが大きい。

【図面の簡単な説明】

【図１】本発明の原理にかかる鍵回復システムの原理を示すブロック図である。

【図２】本発明の鍵回復システムの一実施例を示すブロック図である。

【図３】図２の実施例における回復者装置の動作を示すフローチャートである。

【図４】図２の実施例における鍵回復情報分散装置の動作を示すフローチャートである。

【図５】図２の実施例における鍵回復装置の動作を示すフローチャートである。

【図６】本発明の実施例に用いられる鍵回復情報の一般的フォーマット図である。

【図７】本発明の実施例に用いられる並列方式で権限分散された鍵回復情報を示すフォーマット図である。

【図８】本発明の実施例に用いられる順次方式で権限分散された鍵回復情報のフォーマットを示す図である。

【図９】鍵回復装置の権限が順序付けられて作成された順次方式の鍵回復情報を示す順序方式のフローチャートである。

【図１０】鍵回復情報分散装置に設けられる鍵回復装置ＩＤとそのアクセス方法との対応テーブルである。

【図１１】図２の鍵回復情報分散装置における認証中継部の動作を示すフローチャートである。

10 【図１２】図２の実施例の回復者装置における暗号処理装置処理部のフローチャートである。

【図１３】図２の実施例の鍵回復装置における暗号処理部のフローチャートである。

【図１４】本発明の他の実施例のブロック図である。

【図１５】本発明の他の実施例のブロック図である。

【図１６】本発明の他の実施例のブロック図である。

【図１７】本発明の他の実施例のブロック図である。

【図１８】本発明の他の実施例のブロック図である。

【図１９】本発明の他の実施例のブロック図である。

20 【図２０】本発明の他の実施例のブロック図である。

【図２１】記録媒体を有する本発明を実現するコンピュータ装置のブロック図である。

【図２２】従来例の権限を分散された鍵回復システムのブロック図である。

【符号の説明】

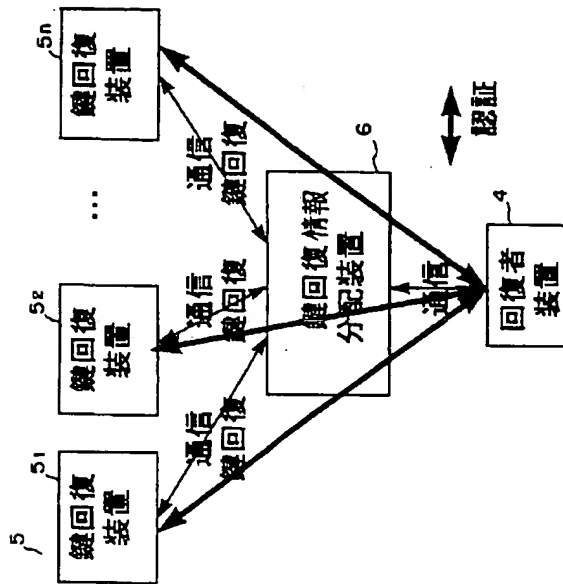
4 回復者装置

5 鍵回復装置

6 鍵回復情報分配装置

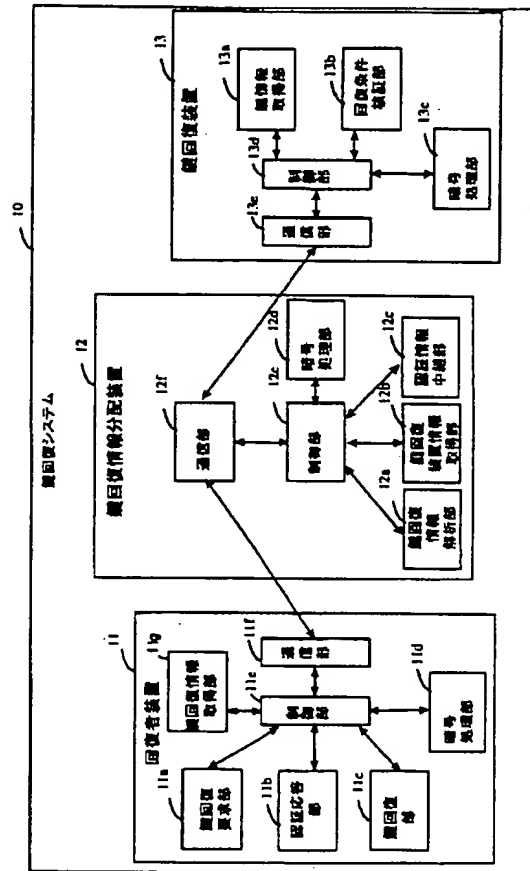
【図1】

本発明の原理にかかる
鍵回復システムの原理を示すブロック図



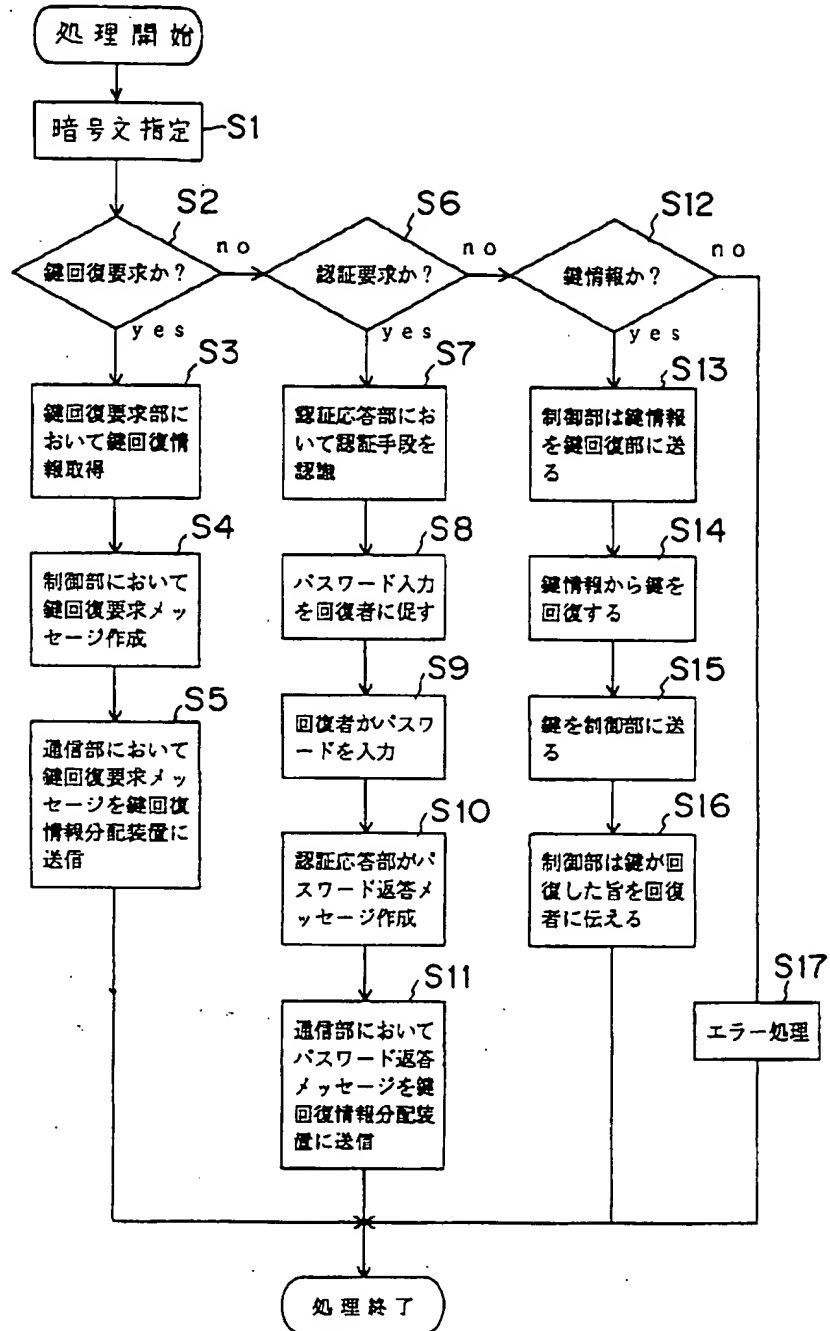
【図2】

本発明の鍵回復システムの一実施を示すブロック図



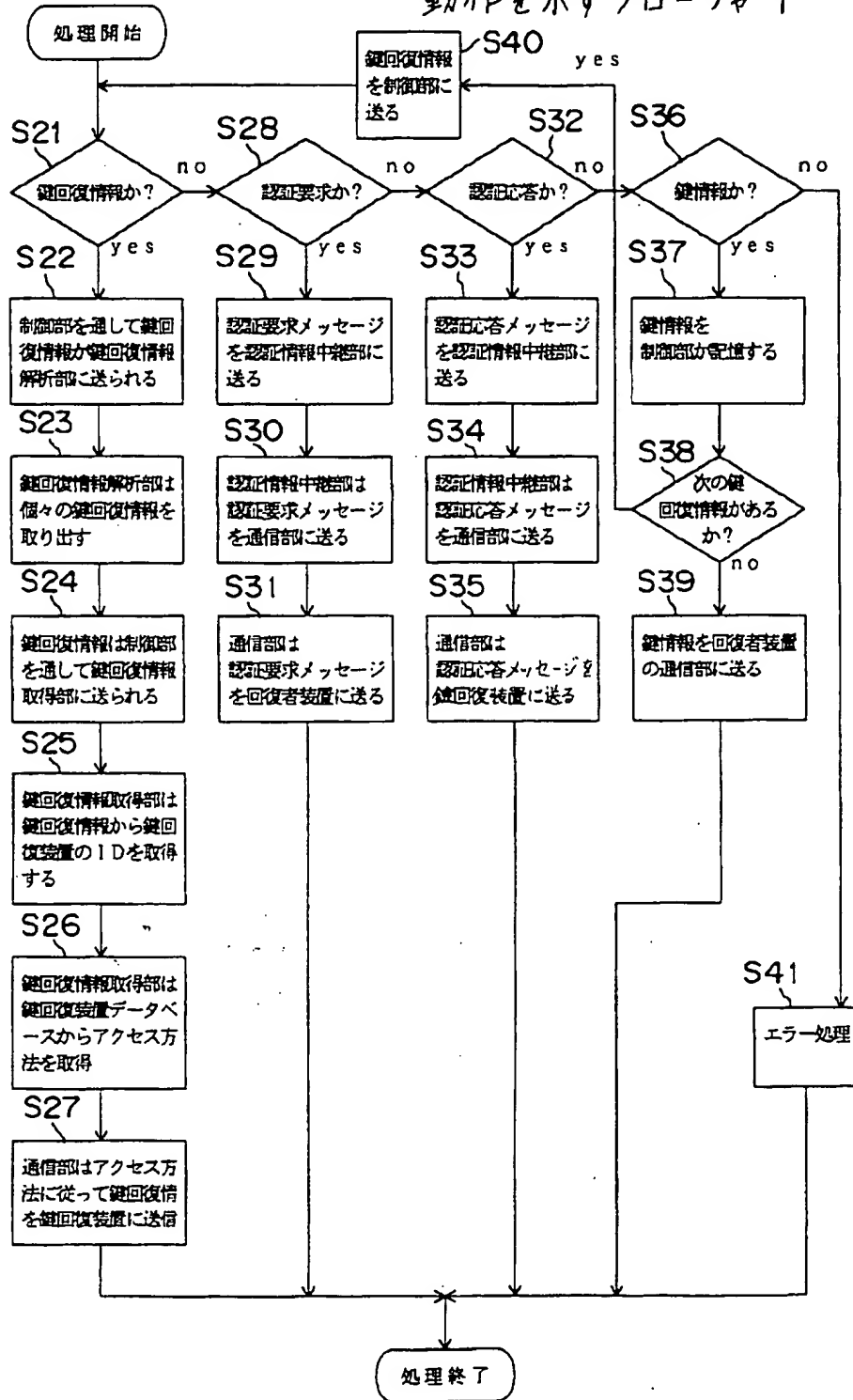
【図3】

図2の実施例における回復者装置の動作を示すフローチャート



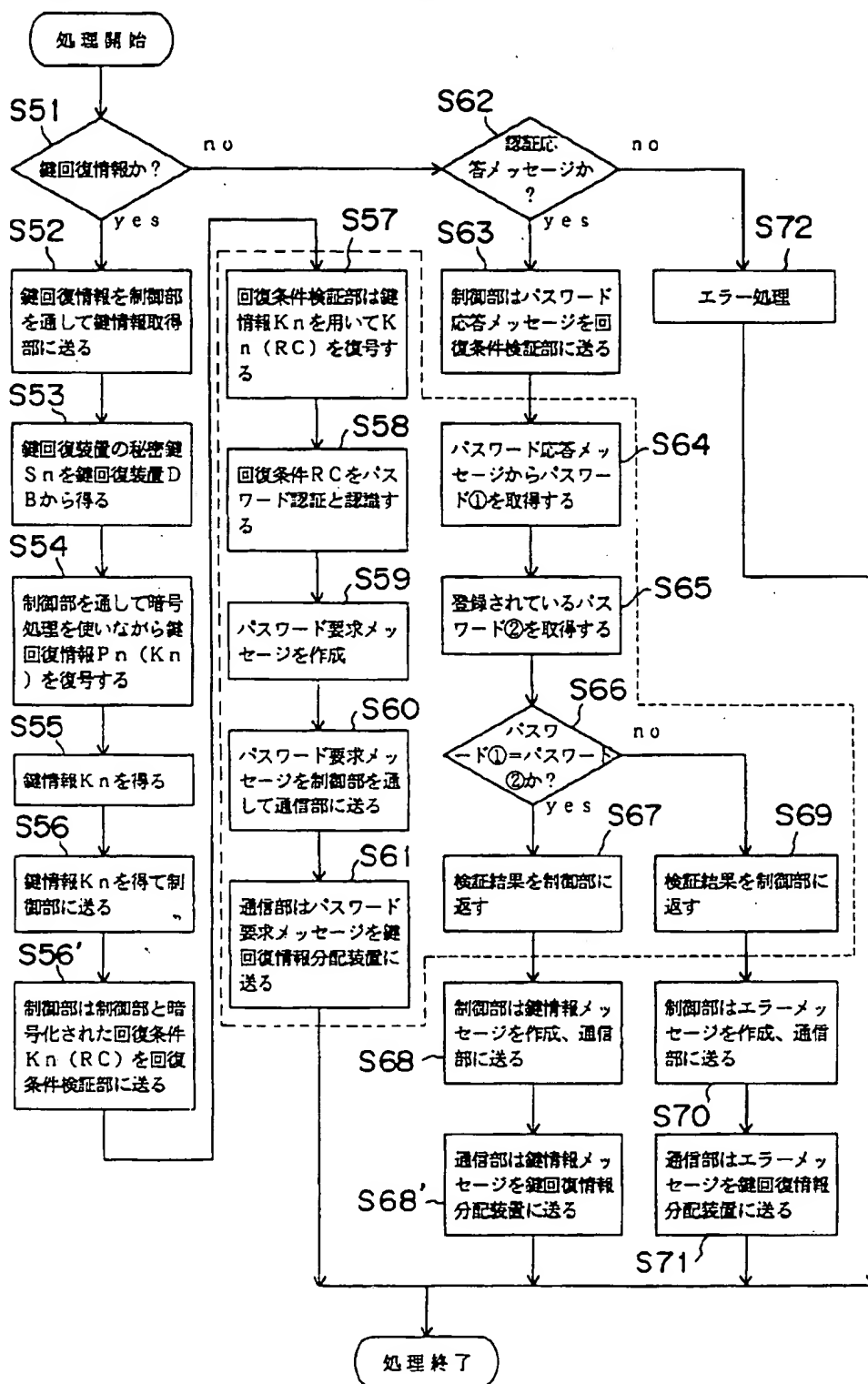
【図4】

図2の実施例における鍵回復情報分散装置の
動作を示すフローチャート



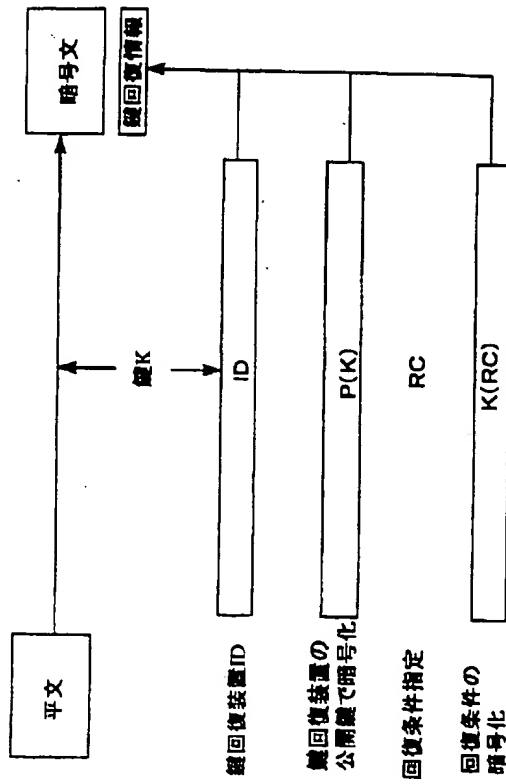
【図5】

図2の実施例における鍵回復装置の動作を示すフローチャート



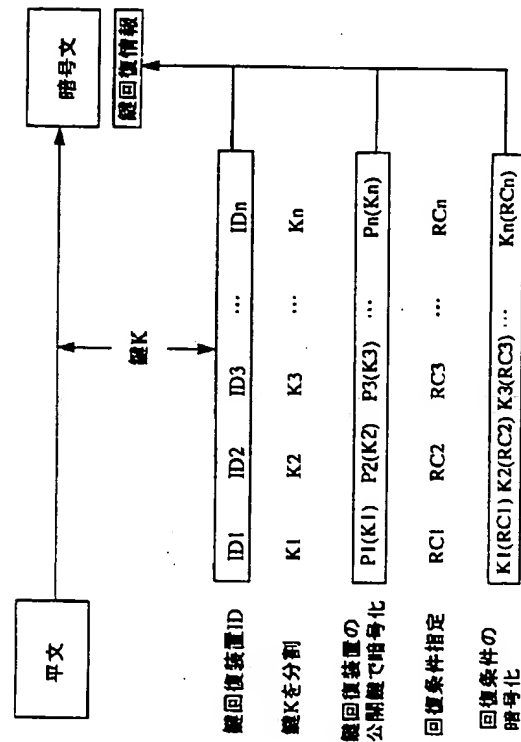
【図6】

本発明の実施例に用いられる
鍵回復情報の一般的フォーマット図



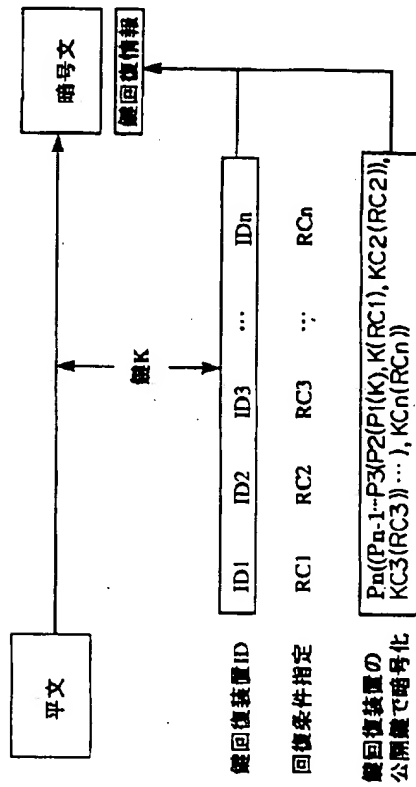
【図7】

本発明の実施例に用いられる並列方式で
権限分散された鍵回復情報のフォーマット図



【図8】

本発明の実施例に用いられる順次方式で
権限分散された鍵回復情報のフォーマットを示す図



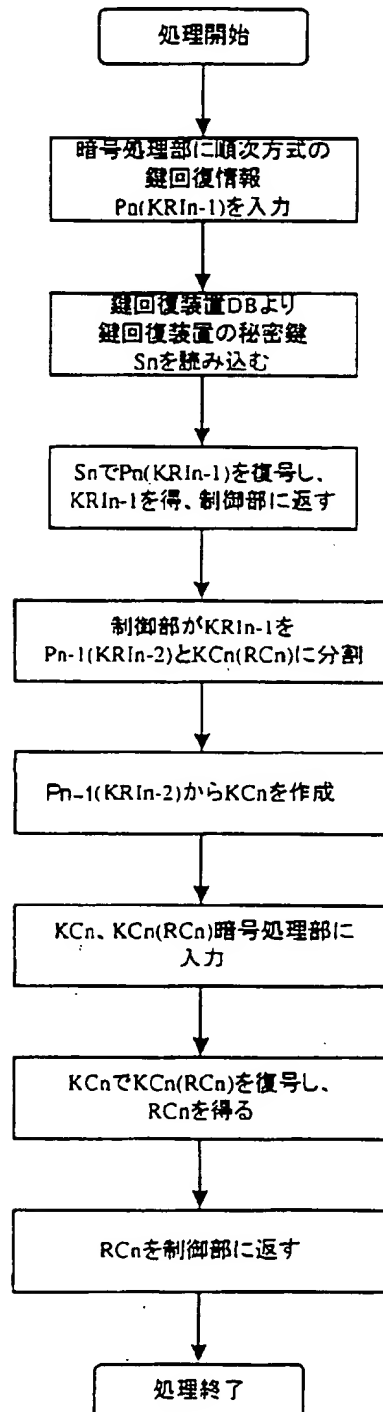
【図10】

鍵回復情報分散装置に設けられる
鍵回復装置 ID とそのアクセス方法との対応テーブル

ID	名前	アクセス先	プロトコル
ID1	A社鍵回復センタ	133.160.30.7	独自プロトコル
ID2	B社鍵回復センタ	kr.or.jp	http
		...	
IDn	N回復センタ	/C=JP/o=KR/	ディレクトリサービス

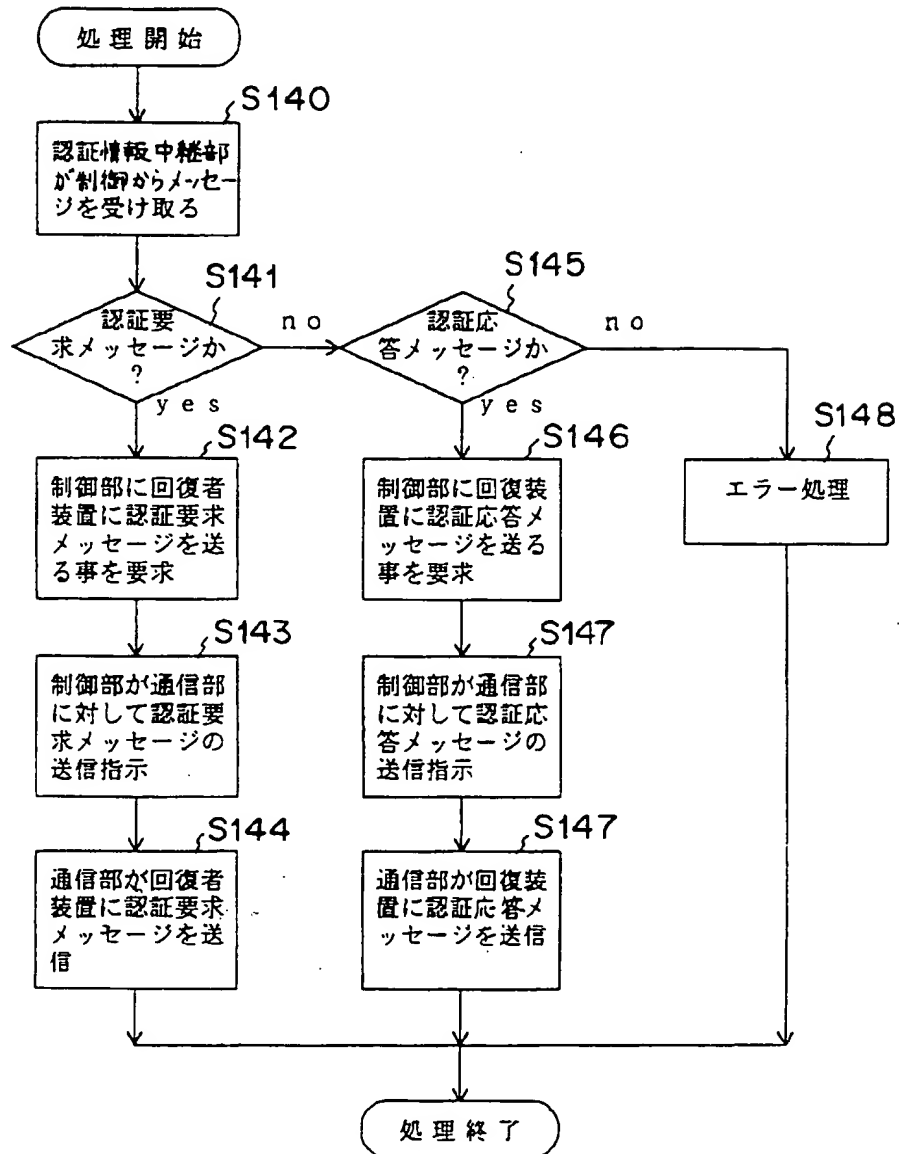
【図9】

鍵回復装置の権限が順序付けられて
作成された順次方式の鍵回復動作を
示すフローチャート



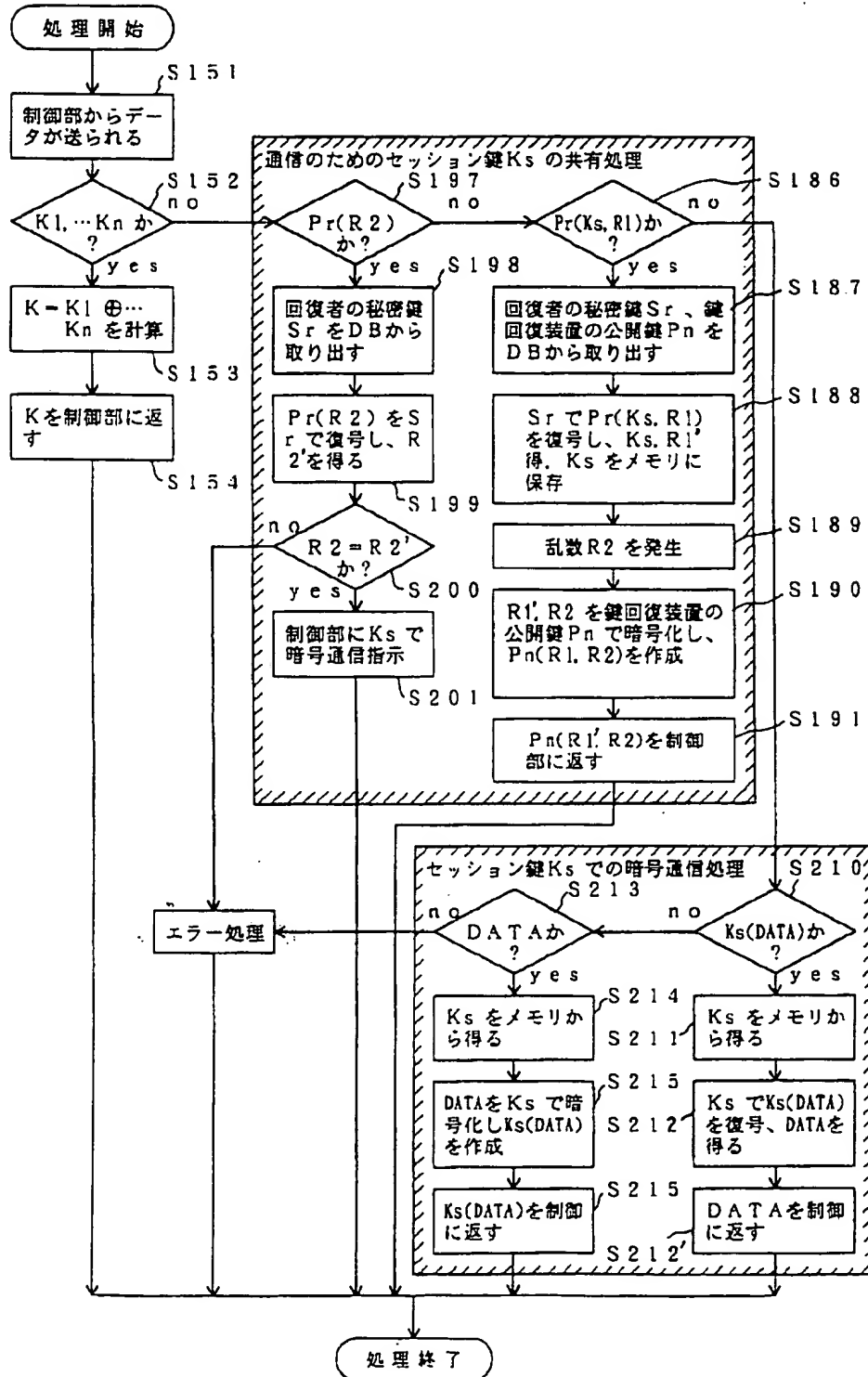
【図11】

図2の鍵回復情報分散装置における
認証中継部の動作を示すフローチャート



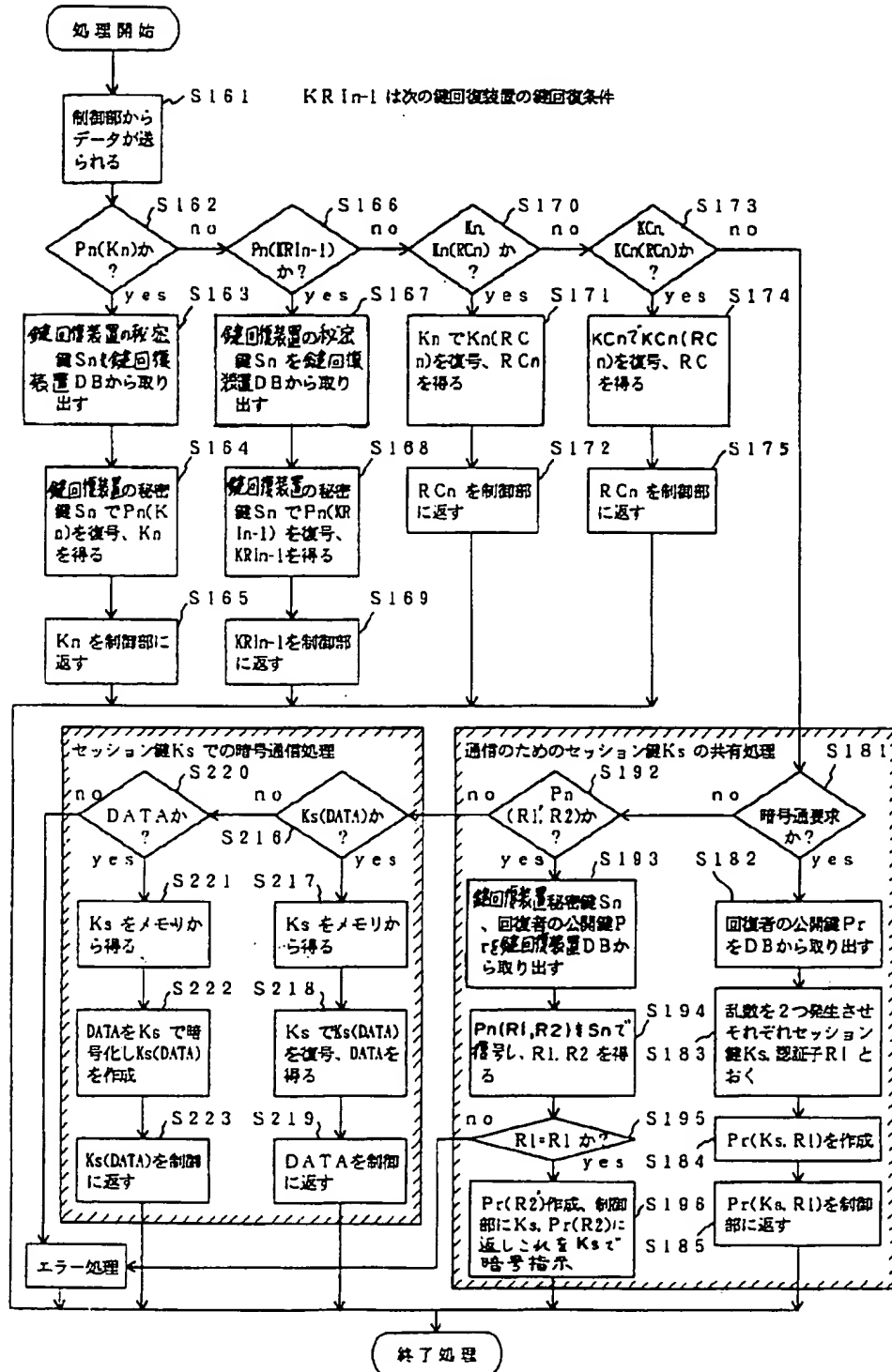
【図12】

図2の実施例の回復者装置における暗号処理装置処理部のフローチャート



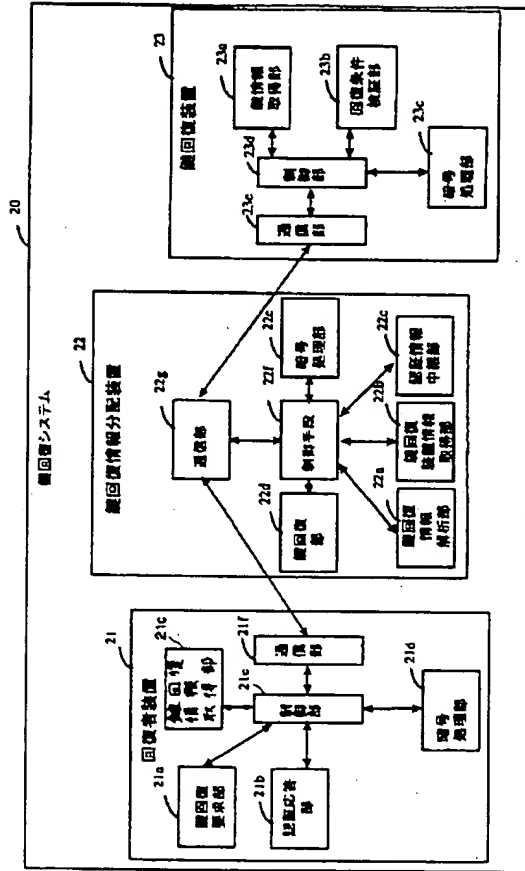
【図13】

図2の実施例の鍵回復装置における暗号処理部のフローチャート



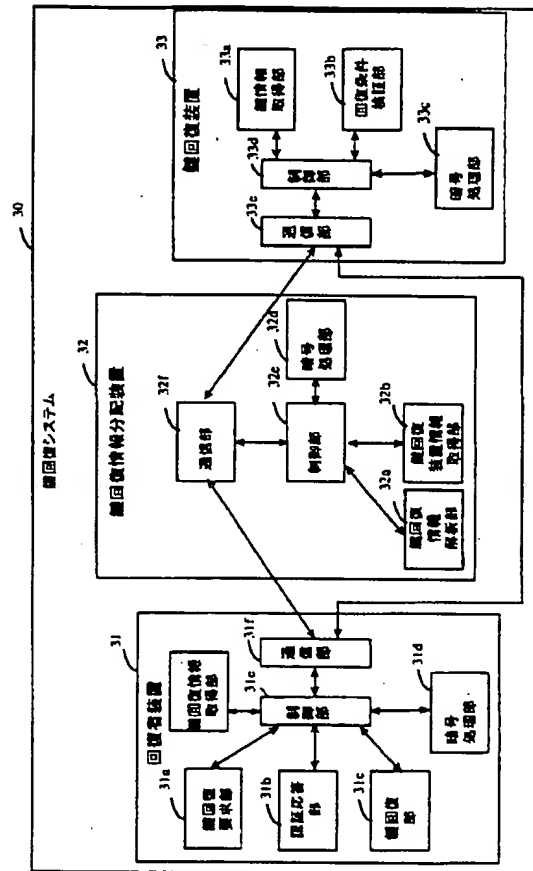
【図14】

本発明の他の実施例のブロック図



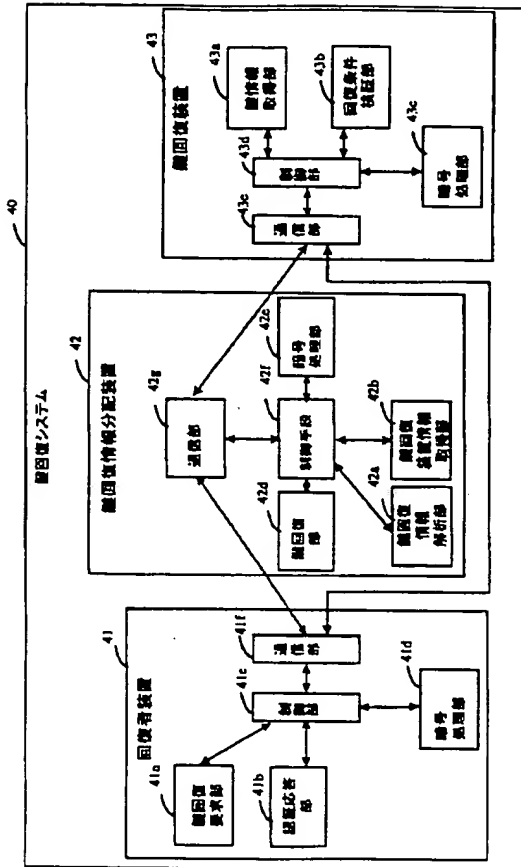
【図15】

本発明の他の実施例のブロック図



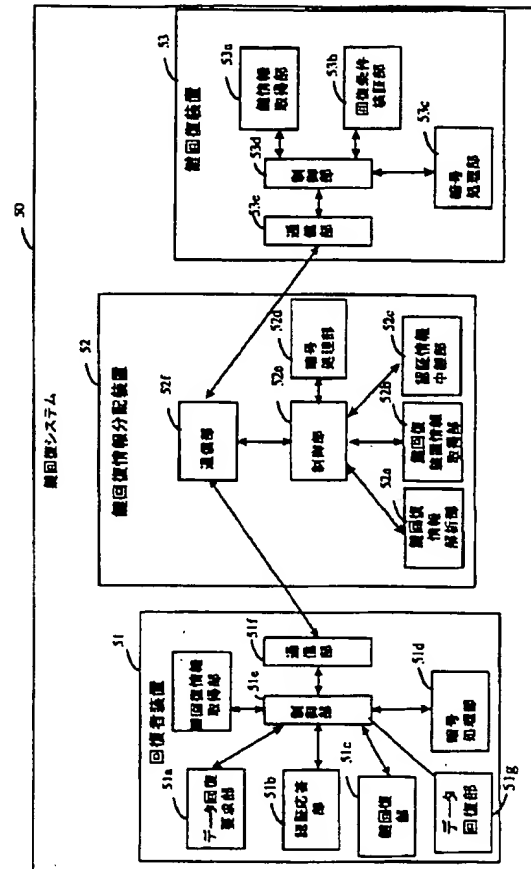
【図16】

本発明の他の実施例のブロック図



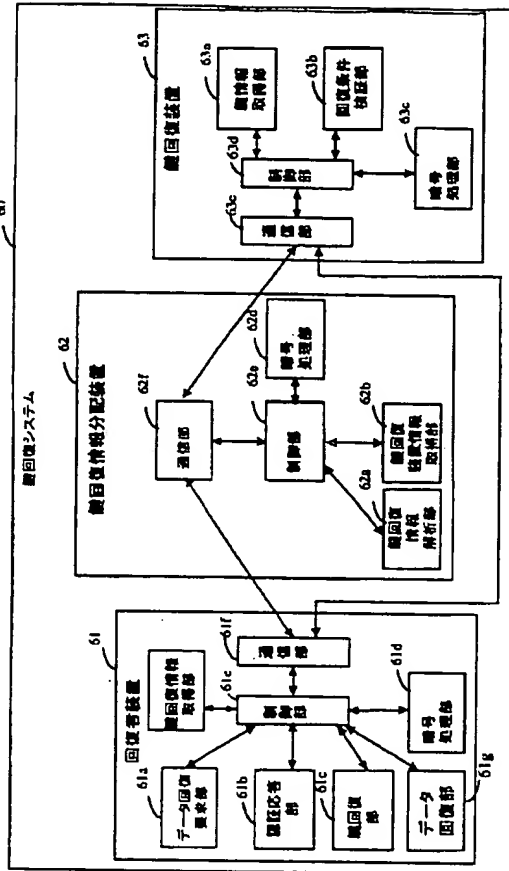
【図17】

本発明の他の実施例のブロック図



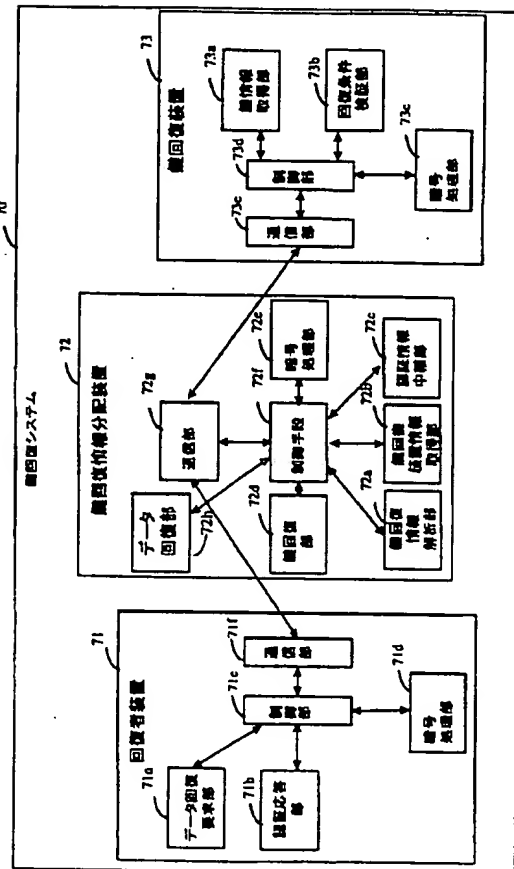
【図18】

本発明の他の実施例のブロック図



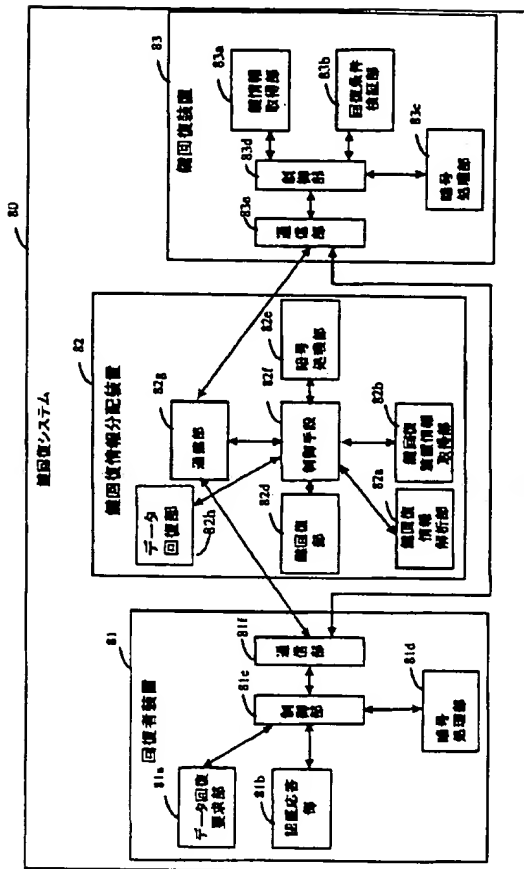
【図19】

本発明の他の実施例のブロック図



【図20】

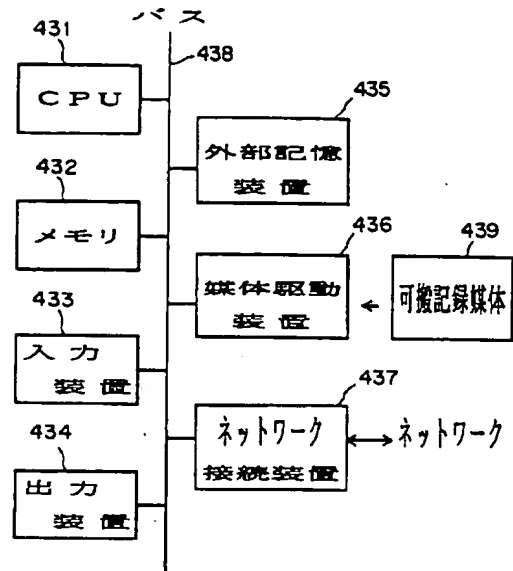
本発明の他の実施例のブロック図



【図21】

記録媒体を有する

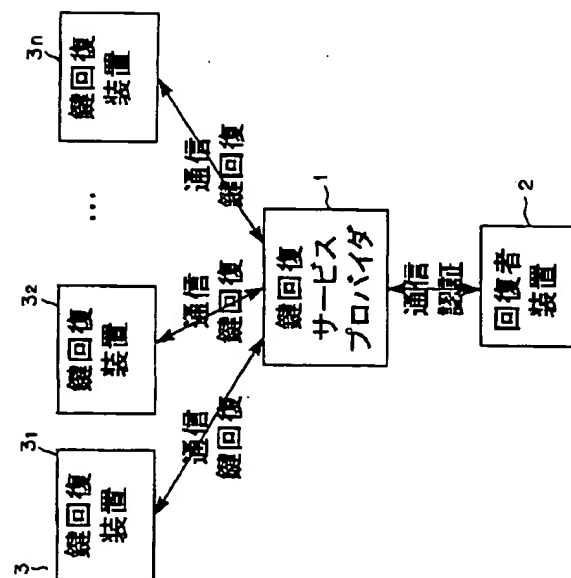
本発明を実現するコンピュータ装置のブロック図



【図22】

従来例の権限を分散された

鍵回復システムのブロック図



フロントページの続き

(72)発明者 安藤 宏幸
神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(72)発明者 森田 一郎
神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(72)発明者 黒田 康嗣
神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(72)発明者 鳥居 直哉
神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(72)発明者 山崎 正史
東京都港区芝五丁目7番1号 日本電気株
式会社内

(72)発明者 宮内 宏
東京都港区芝五丁目7番1号 日本電気株
式会社内

(72)発明者 佐古 和恵
東京都港区芝五丁目7番1号 日本電気株
式会社内

(72)発明者 道明 誠一
神奈川県川崎市麻生区王禅寺1099番地 株
式会社日立製作所システム開発研究所内

(72)発明者 土屋 宏嘉
神奈川県横浜市戸塚区戸塚町5030番地 株
式会社日立製作所ソフトウェア開発本部内

(72)発明者 菅野 聖子
神奈川県横浜市戸塚区戸塚町180番地 日
立通信システム株式会社内